Avira

Exchange Security

Benutzerhandbuch

Avira Exchange Security

Inhaltsverzeichnis

1 Quickstart 5
1.1 Installation auf einem Exchange-Server 5
1.2 Starten der Avira Exchange Security Management Console 5
1.3 Konfiguration in der Avira Exchange Security Management Console 6
1.3.1 Notwendige Schritte in der Basiskonfiguration 7
1.3.2 Notwendige Schritte in der Richtlinien-Konfiguration 7
1.3.3 Empfehlenswerte Schritte in der Basiskonfiguration 7
1.3.4 Virenprüfung der Exchange Datenbanken 8
1.4 Beobachtung der Daten im Avira Monitor 8
2 Installation 9
2.1 Systemvoraussetzungen 9
2.2 Installation von Avira Exchange Security auf einem Exchange-Server 10
2.3 Deinstallation von Avira Exchange Security 15
3 Produktbausteine 16
3.1 Avira Exchange Security Management Console 16
3.1.1 Zugriffsmethoden 16
3.1.2 Betriebsmodi 16
3.2 Avira Exchange Security Server 17
3.2.1 Der Transport-Agent 17
3.2.2 Der Avira Exchange Security Dienst = Enterprise Message Handler (EMH) 18
3.2.3 Quarantäne 18
3.2.4 Das Active Directory/LDIF 19
3.2.5 Komprimierte Dateien/Archive - Avira Exchange Security Unpacker 20
3.3 Die Konfigurationsdatei von Avira Exchange Security 20
3.3.1 Verwendung einer benutzerdefinierten Konfigurationsdatei 21
4 Avira Monitor 22
4.1 Zugriff auf den Avira Monitor einrichten 22
4.2 Verwendung des Avira Monitor 22
4.3 Quarantänen verwenden 23
4.4 Emails aus der Quarantäne senden 24
4.5 Absender einer Adressliste hinzufügen 26
4.6 Domain einer Adressliste hinzufügen 26
4.7 BADMAIL 27
4.8 Details einer unter Quarantäne gestellten Email 27
4.8.1 Email-Details 27
4.8.2 Quarantäne-Verarbeitungsprotokoll 28
4.8.3 Quarantäne-Details 29
4.9 Details in der IS-Quarantäne 30
4.9.1 Email-Details in der IS-Quarantäne 30
4.9.2 IS Quarantäne-Verarbeitungsprotokoll 31
4.10 Quarantäne-Schaltflächen 32
4.11 Avira Exchange Security-Statistiken 33
4.12 Erstellung von Statistiken 33
5 Avira Scan Engine 34
5.1 Avira Prüfung-Jobs 34

5.1.1 Avira Scan Engine konfigurieren und aktivieren....35
5.1.2 Virenprüfung aktivieren....38
5.2 Suche im Informationsspeicher-Jobs....45
5.2.1 Informationsspeicher-Status....46
5.2.2 Informationsspeicherscan neu starten....47
5.2.3 Einen Suche im Informationsspeicher-Job aktivieren....47
5.3 Avira geschützte Anhangserkennung....53
5.3.1 Einstellungen für einen Avira geschützte Anhangserkennung-Job....54
5.4 Avira Anhangsfilterung-Jobs....55
5.4.1 Fingerprints....56
5.4.2 Videodateien blockieren....57
5.5 Avira Email-Größenfilterung-Jobs....60
5.5.1 Email-Größe beschränken....61
5.6 Avira Anhangs-/Größenfilterung Jobs....64
5.6.1 Office-Dateien blockieren....65
6 Avira Email-Filter....70
6.1 Adressprüfung....70
6.1.1 Absender oder Empfänger blockieren....71
6.2 Prüfung der Textinhalte mithilfe von Wortlisten....74
6.2.1 Wortlisten erstellen....74
6.2.2 Textsuche in Wortlisten....76
6.2.3 Anstößige Inhalte blockieren....78
6.2.4 Schwellwertberechnung bei Inhaltsfilterung....80
6.3 Anzahl der Empfänger einschränken....81
6.4 Erweiterte Email-Filter-Einstellungen....85
6.4.1 Definitive Kriterien....85
6.4.2 Kombinierte Kriterien....88
6.4.3 Erweiterte Email-Filterung....93
6.4.4 Email-Filter manuell konfigurieren....104
7 Detaillierte Konfiguration....106
7.1 Basiskonfiguration....106
7.1.1 Konfigurationsreports erstellen....106
7.1.2 Konfiguration importieren....107
7.1.3 Standardeinstellungen für alle Server....108
7.1.4 Erstellen eines Avira Server....111
7.1.5 Einstellungen für einen individuellen Avira Server....111
7.2 Datenbankverbindungen....118
7.2.1 Voraussetzungen für Datenbankverbindungen....119
7.2.2 Datenbankverbindung konfigurieren....119
7.2.3 Beispiel einer ADO-String-Konfiguration....121
7.2.4 Zentrale Whitelists konfigurieren....122
7.2.5 Quarantäne-Datenbank konfigurieren....122
7.2.6 Handhabung von SQL-Server-Problemen....123
7.3 Adresslisten....124
7.3.1 Adresslisten erstellen....124
7.3.2 Adressliste löschen....126
7.3.3 Adresslisten im Job verwenden....126
7.3.4 Adresseinstellungen wenn auf Viren geprüft wird....128
7.3.5 Adresseinstellungen bei blockierten Dateianhängen....129

7.4 Vorlagen ... 130
7.4.1 Benachrichtigungsvorlagen erstellen ... 130
7.4.2 Liste der Benachrichtigungsvariablen ... 131
7.5 Konfiguration der Quarantäne ... 139
7.5.1 Eine neue Quarantäne erstellen ... 140
7.5.2 Quarantäne konfigurieren ... 140
7.5.3 Beispiel einer geschäftskritischen Quarantäne ... 142
7.5.4 Quarantäne-Zusammenfassungen ... 143
7.5.5 Sammelbenachrichtigung erstellen ... 143
7.6 Utility-Einstellungen ... 148
7.7 Konfiguration der Richtlinien-Konfiguration ... 149
7.7.1 Beispiel für eine Unternehmensrichtlinie ... 149
7.7.2 Jobarten ... 149
7.7.3 Job-Bedingungen ... 151
7.7.4 Job-Aktionen ... 152
8 Schaltflächen der Symbolleiste ... 153
9 Bedeutung der Symbole ... 154
10 Supportinformationen ... 157

1 Quickstart

Die Kurzanleitung für Avira Exchange Security.

1.1 Installation auf einem Exchange-Server

1. Zur Installation von Avira Exchange Security führen Sie bitte einen Doppelklick auf die Installationsdatei aus.
   - *avira_exchange_security_64bit.exe*
2. Folgen Sie den Anweisungen des Installationsassistenten bis die Installation abgeschlossen ist.

   Falls Sie kein anderes Installationsverzeichnis angeben, wird Avira Exchange Security im folgenden Standardverzeichnis installiert:

   für die 64-Bit Version:

   - *C:\Program Files(x86)\Avira\Avira Exchange Security* (Englisch)
   - *C:\Programme(x86)\Avira\Avira Exchange Security* (Deutsch)
3. Deaktivieren Sie die Echtzeit- oder On-Access-Scanner verwendeter Virenscanner für das Verzeichnis ...*\Avira\Avira Exchange Security\AppData*.
4. Starten Sie Avira Exchange Security Management Console.
5. Nehmen Sie die empfohlenen Einstellungen für die **Basiskonfiguration** und die **Richtlinien-Konfiguration** vor.

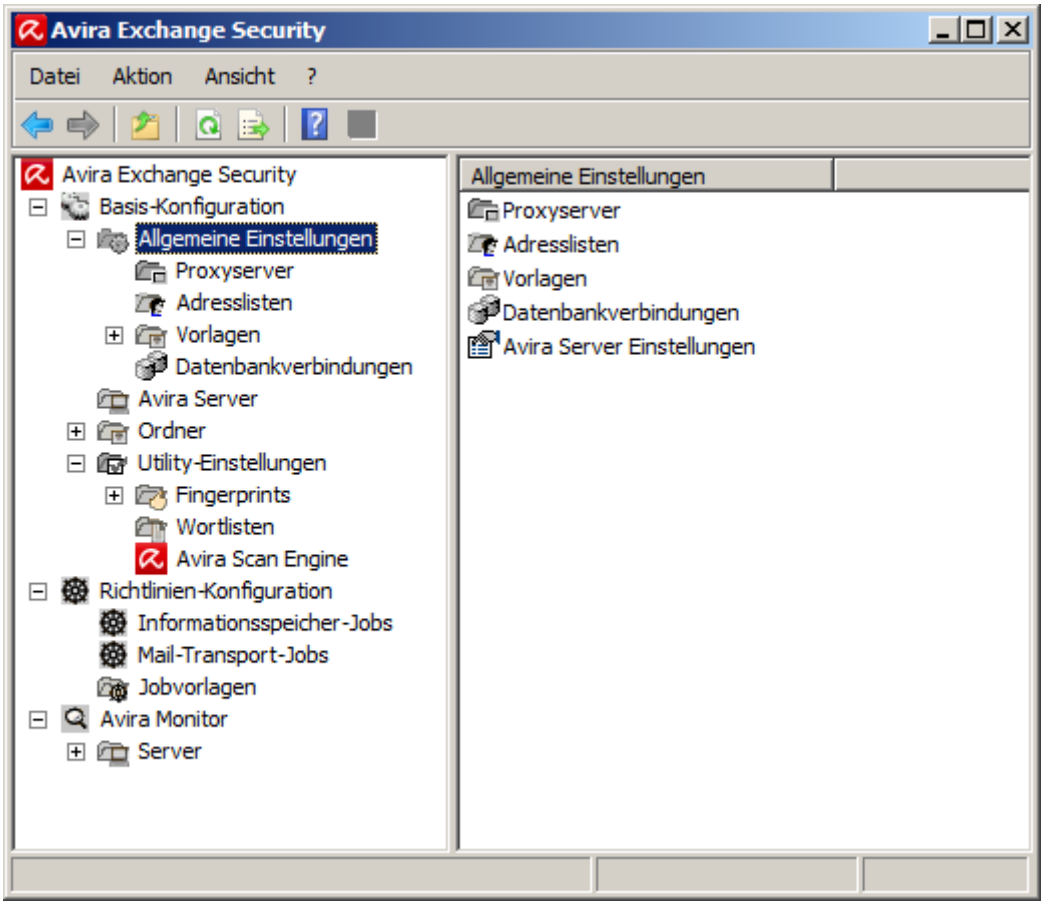
Verwandte Themen:

Notwendige Schritte in der Basiskonfiguration - Seite 7
Notwendige Schritte in der Richtlinien-Konfiguration - Seite 7

1.2 Starten der Avira Exchange Security Management Console

Avira Exchange Security ist ein Serverprodukt, das durch die Avira Exchange Security Management Console konfiguriert wird. Damit Avira Exchange Security funktioniert, muss der Dienst Avira Exchange Security gestartet sein.

1. Um die Konsole zu starten, klicken Sie **Start > Programs > Avira > Avira Exchange Security > Avira Exchange Security Management Console**.



2. Um Änderungen an der Konfiguration der Konsole zu speichern, klicken Sie die Schaltfläche **Konfiguration speichern** .

   Nicht gespeicherte Änderungen werden durch (*) am obersten Knoten angezeigt.

   Die Konfiguration wird in der Datei *ConfigData.xml* gespeichert, die im Verzeichnis ...*Avira \Avira Exchange Security\Config* abgelegt ist.

Verwandte Themen:

Der Avira Exchange Security Dienst = Enterprise Message Handler (EMH) - Seite 18
Schaltflächen der Symbolleiste - Seite 153
Bedeutung der Symbole - Seite 154

1.3 Konfiguration in der Avira Exchange Security Management Console

Im Anschluss an die Installation von Avira Exchange Security legen Sie die Konfiguration in der Konsole fest.

1.3.1 Notwendige Schritte in der Basiskonfiguration

In der **Basiskonfiguration** definieren Sie die gültigen Server, Email-Adressen, gemeinsamen Vorlagen und Utility-Einstellungen.

> Überprüfen Sie unter **Basiskonfiguration** > **Allgemeine Einstellungen** > **Avira Server Einstellungen** auf der Registerkarte **Email-Adressen** die Einträge für die **Administratoren** und die **Internen Domänen**.

Verwandte Themen:

Standardeinstellungen für alle Server - Seite 108

1.3.2 Notwendige Schritte in der Richtlinien-Konfiguration

In der **Richtlinien-Konfiguration** definieren und aktivieren Sie die gewünschten Jobs gemäß Ihren Firmenrichtlinien. D.h. Jobs sind nichts anderes als regelbasierte Maßnahmen oder Aktionen, die auf den Email-Verkehr angewandt werden.

Es ist wichtig, zwischen zwei Kategorien für Jobs zu unterscheiden.

- Jobs für die **Avira Scan Engine**, die nach Viren, Malware oder schädlichen Skripten suchen oder Emails nach Größe und/oder Typ des Dateianhanges filtern.
- Jobs für die **Avira Email-Filter**, anhand derer Emails nach einer Reihe von Kriterien (z.B. Adressen, Wörter, Bilder) gefiltert werden können.

Um einen neuen Job anzulegen, führen sie folgende Schritte aus:

1. Suchen Sie sich unter **Jobvorlagen** die gewünschte Vorlage aus.
2. Markieren Sie die Vorlage und ziehen Sie diese in den Ordner **Mail-Transport-Jobs**.
3. Konfigurieren Sie den Namen und die Eigenschaften dieses Jobs und schalten Sie den Job unter Eigenschaften aktiv. (*Aktiv: Ja*).

Hinweis
Achten Sie auf die Abarbeitungsreihenfolge der Jobs.

4. Klicken Sie **Konfiguration speichern**, um Ihre Einstellungen zu speichern.

1.3.3 Empfehlenswerte Schritte in der Basiskonfiguration

Es ist empfehlenswert, in der **Basiskonfiguration** individuelle Einstellungen für Adresslisten, Vorlagen usw. vorzunehmen. Diese Einstellungen sind für einen Testbetrieb aber nicht zwingend erforderlich.

1. Konfigurieren Sie die **Adresslisten** (für die Auswahl in den Job-Regeln) unter **Allgemeine Einstellungen**.
2. Ändern Sie ggf. die Standard-Vorlagen unter **Allgemeine Einstellungen**.
3. Konfigurieren Sie unter **Utility-Einstellungen** das benötigte Zubehör wie Wortlisten, Fingerprints und Virenscanner.

1.3.4 Virenprüfung der Exchange Datenbanken

In **Richtlinien-Konfiguration** > **Informationsspeicher-Jobs** können Sie für jeden Avira Server getrennt die entsprechenden Einstellungen vornehmen.

Informationsspeicher-Jobs können nicht selbst angelegt werden. Sobald Sie einen neuen Server hinzugefügt haben, steht automatisch ein entsprechender Informationsspeicher-Job zur Verfügung.

Wenn Sie den Server wieder entfernen, wird auch der Informationsspeicher-Job gelöscht.

Verwandte Themen:

Suche im Informationsspeicher-Jobs - Seite 45

1.4 Beobachtung der Daten im Avira Monitor

Nach dem Speichern Ihrer Einstellungen überwachen Sie den laufenden Betrieb von Avira Exchange Security mit dem **Avira Monitor**.

Im **Avira Monitor** können Sie die aktuellen "Live-Daten" beobachten und zum Beispiel die Quarantänen der konfigurierten Server administrieren.

Verwandte Themen:

Avira Monitor - Seite 22

2 Installation

2.1 Systemvoraussetzungen

Mindestsystemvoraussetzungen für die Avira Exchange Security-Installation

Hinweis

Für Informationen über Cluster-Installation wenden Sie sich bitte an den Avira-Support.

Warnung

Deaktivieren Sie die Echtzeit- oder On-Access-Scanner verwendeter Virenscanner für das Verzeichnis ...*Avira**Avira Exchange Security**AppData*.

- Betriebssysteme (64 Bit):
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
- Exchange Server:
  - MS Exchange Server 2007 SP1 Update-Rollup 4 (64 Bit) (oder höher, d. h. SP2/SP3 einschließlich aller bisherigen Rollups)
  - MS Exchange Server 2010 (64 Bit) (oder höher, d. h. SP1/ SP2 einschließlich aller bisherigen Rollups)
  - MS Exchange Server 2013 (64 Bit)
- RAM: Exchange-Empfehlung + zusätzlich 64 MB
- Festplatte: Mindestens 400 MB für die Installation
- CD-ROM-Laufwerk oder Netzwerkzugriff
- Microsoft .NET Framework 3.5
- 100 MB für die Ereignisprotokollierung empfohlen
- Internetzugang für Engine-Updates (Scan Engine und Email Filter Engine)
- Benutzerrechte: Im Active Directory registrierte Benutzer mit komplettem Lesezugriff auf das Active Directory.
- Betriebssysteme für Avira Exchange Security Management Console:
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows XP Professional
  - Windows Vista
  - Windows 7

- Windows 8

2.2 Installation von Avira Exchange Security auf einem Exchange-Server

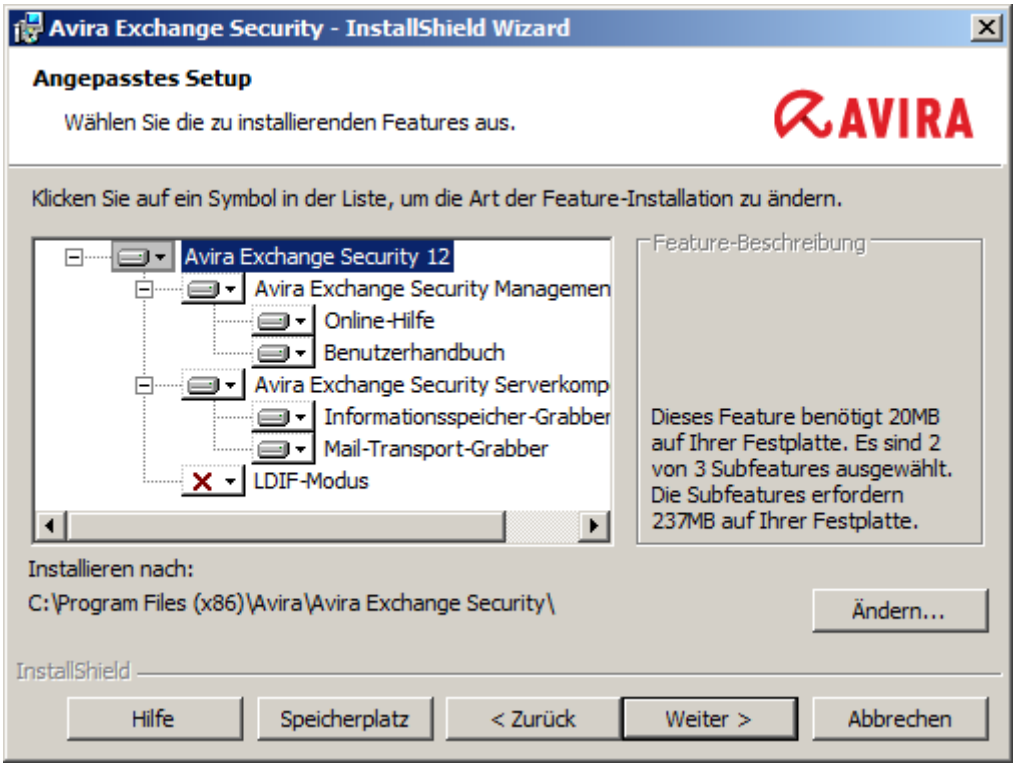
1. Zur Installation von Avira Exchange Security führen Sie bitte einen Doppelklick auf die Installationsdatei aus. Ein Beispiel:
   avira_exchange_security_64bit.exe
2. Wählen Sie die Setup-Sprache aus und klicken Sie anschließend **Weiter**.
3. Wählen Sie das Betriebssystem und die Produktsprache aus.

   Die ausgewählte Produktsprache gilt für die Produktoberfläche und für die Anwenderbenachrichtigungen, die von Avira Exchange Security an die Benutzer verschickt werden.

Avira Exchange Security - InstallShield Wizard
Sprachauswahl
Wählen Sie die Plattform und die Sprache für das Produkt
AVIRA
Wählen Sie die Sprache für die Management Konsole und Anwenderbenachrichtigungen aus:
Deutsch
InstallShield
< Zurück
Weiter >
Abbrechen

4. Akzeptieren Sie im nächsten Dialogfenster die *Lizenzvereinbarung*, um fortfahren zu können und klicken Sie **Weiter**.
5. Wählen Sie aus, welche Programmkomponenten Sie installieren wollen.

   Mit dieser Auswahl werden alle Serverkomponenten und die Avira Exchange Security Management Console installiert.

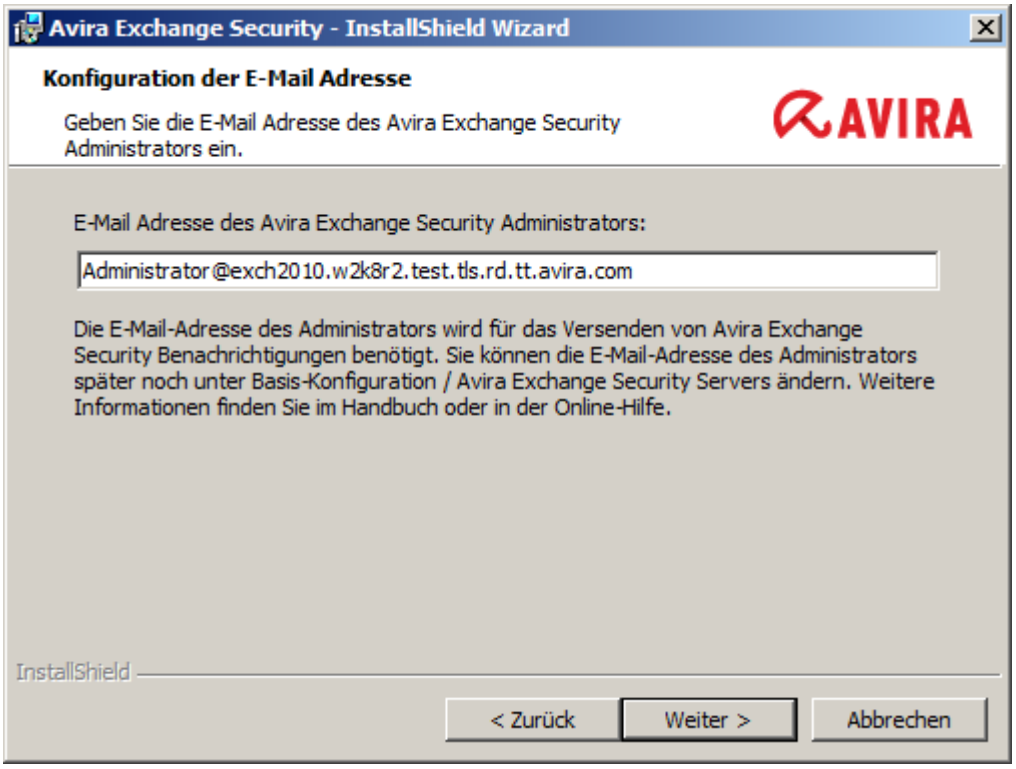


Sollte sich eine andere aktive Informationsspeicher-Scan-Anwendung, ausgenommen Avira Exchange Security, auf dem Server befinden, ist die Informationsspeicher-Scan-Funktion inaktiv. Wenn Sie den Informationsspeicher-Scan benutzen wollen, müssen Sie zuerst die andere Anwendung deinstallieren.

6. Klicken Sie **Weiter**.

Sie werden nach dem Speicherort der Konfigurationsdatei gefragt.

7. Wenn Sie Avira Exchange Security nicht auf mehreren Servern betreiben und dabei zentral mit einer Konfiguration administrieren möchten, bestätigen Sie die Voreinstellung und klicken Sie **Weiter**.

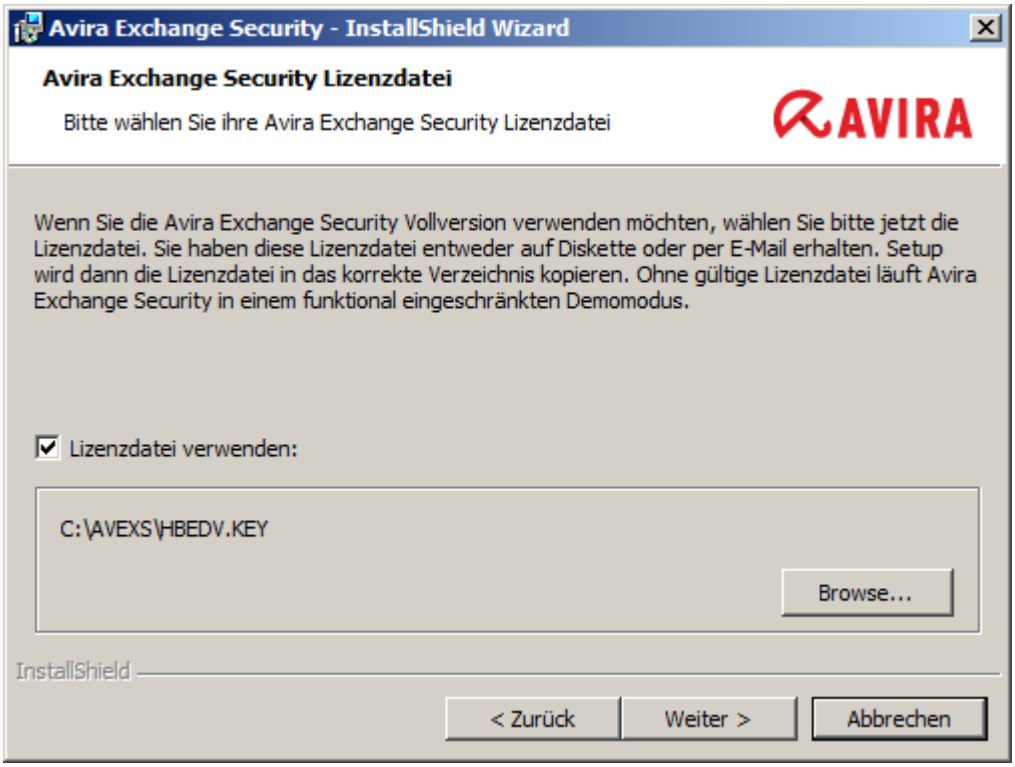

Avira Exchange Security - InstallShield Wizard
Konfiguration der E-Mail Adresse
Geben Sie die E-Mail Adresse des Avira Exchange Security Administrators ein.
AVIRA
E-Mail Adresse des Avira Exchange Security Administrators:
Administrator@exch2010.w2k8r2.test.tls.rd.tt.avira.com
Die E-Mail-Adresse des Administrators wird für das Versenden von Avira Exchange Security Benachrichtigungen benötigt. Sie können die E-Mail-Adresse des Administrators später noch unter Basis-Konfiguration / Avira Exchange Security Servers ändern. Weitere Informationen finden Sie im Handbuch oder in der Online-Hilfe.
InstallShield
< Zurück
Weiter >
Abbrechen

8. Legen Sie die Email-Adresse des Administrators fest und klicken Sie **Weiter**.
9. Wenn Sie einen Proxy-Server für das Avira-Update verwenden, aktivieren Sie das Kontrollkästchen und nehmen Sie die Proxyeinstellungen zu IP-Adresse, Port, Benutzer und Passwort vor. Das Passwort wird im Klartext abgespeichert.

Avira Exchange Security - InstallShield Wizard
Proxy Server Einstellungen
Geben Sie die Informationen ihres Proxy Servers ein
Folgende Proxy-Einstellungen werden zur Aktualisierung der in Avira Exchange Security integrierten Antivirus und Antispam Engines verwendet. Die Einstellungen können hier angegeben werden, oder Sie können dies später in der Administrations-Konsole nachholen.
Proxy Server verwenden
Proxy Adresse:
ihr_proxy@domain.de
Port:
8080
Benutzer:
administrator
Passwort:
InstallShield
< Zurück
Weiter >
Abbrechen

10. Klicken Sie **Weiter**.

Sie werden nach der Lizenzdatei gefragt.


Avira Exchange Security - InstallShield Wizard
Avira Exchange Security Lizenzdatei
Bitte wählen Sie ihre Avira Exchange Security Lizenzdatei
Wenn Sie die Avira Exchange Security Vollversion verwenden möchten, wählen Sie bitte jetzt die Lizenzdatei. Sie haben diese Lizenzdatei entweder auf Diskette oder per E-Mail erhalten. Setup wird dann die Lizenzdatei in das korrekte Verzeichnis kopieren. Ohne gültige Lizenzdatei läuft Avira Exchange Security in einem funktional eingeschränkten Demomodus.
Lizenzdatei verwenden:
C:\AVEXS\HBEDV.KEY
Browse...
InstallShield
< Zurück
Weiter >
Abbrechen

11. Aktivieren Sie die Option **Lizenzdatei verwenden** und benutzen Sie **Browse**, um den Pfad zur Lizenzdatei festzustellen.

12. Klicken Sie **Weiter**.

Sie erhalten nun eine Zusammenfassung Ihrer Einstellungen.

Avira Exchange Security - InstallShield Wizard
Bereit das Programm zu installieren
Der Assistent ist bereit, die Installation zu beginnen.
Klicken Sie "Installieren", um mit der Installation zu beginnen.
Klicken Sie auf "Zurück", wenn Sie Ihre Installationseinstellungen überprüfen oder ändern wollen. Klicken Sie auf "Abbrechen", um den Assistenten zu beenden.
ACHTUNG:
In seltenen Fällen kann nach der Installation ein Windows-Neustart erforderlich sein. Die Systemvoraussetzungen für den Betrieb der Avira Exchange Security werden mit Hilfe des Eicar-Test-Virus untersucht. Bitte stellen Sie sicher, dass eventuelle Real-Time bzw. On-Access Scanner für das Verzeichnis "C:\Program Files (x86)\Avira\Avira Exchange Security\AviraData\" deaktiviert sind!
Ausgewählte Komponenten:
Avira Exchange Security Serverkomponenten
Informationsspeicher-Grabber
Mail-Transport-Grabber
InstallShield
< Zurück
Installieren
Abbrechen

13. Deaktivieren Sie jetzt die Echtzeit- oder On-Access-Scanner verwendeter Virenscanner für das Verzeichnis ...*Avira\Avira Exchange Security\AppData*, falls Sie das noch nicht getan haben.
14. Überprüfen Sie Ihre Konfigurationseinstellungen. Diese Einstellungen werden als Standardeinstellungen in die Konfiguration des Avira Exchange Security Server übernommen.
15. Folgen Sie weiter den Anweisungen und klicken Sie **Installieren**.
    Avira Exchange Security wird in folgendes Verzeichnis installiert (Beispiel): *C:\Program Files(x86)\Avira\Avira Exchange Security*
16. Klicken Sie **Fertigstellen**.

Avira Exchange Security wurde erfolgreich installiert. Der Virenscanner ist fertig konfiguriert und sofort einsatzfähig. Dazu stellen wir einen Job für die Virenprüfung mit Avira zur Verfügung, den Sie einfach aktivieren können.

Verwandte Themen:

Standardeinstellungen für alle Server - Seite 108
Avira Scan Engine konfigurieren und aktivieren - Seite 35

2.3 Deinstallation von Avira Exchange Security

1. Klicken Sie **Start** > **Systemsteuerung** > **Programme und Funktionen**.
2. Wählen Sie Avira Exchange Security aus.
3. Wählen Sie **Ändern**.
4. Wählen Sie **Deinstallieren** aus.
   Das Setup wird aufgerufen und deinstalliert **Avira Exchange Security**.

3 Produktbausteine

Avira Exchange Security besteht aus mehreren Komponenten.

3.1 Avira Exchange Security Management Console

Die Avira Exchange Security Management Console ist die Benutzeroberfläche, über die Avira Exchange Security konfiguriert und administriert wird. Es handelt sich hierbei um ein so genanntes "Snap-In" für die MMC.

Mit der Konsole können sowohl einzelne Exchange-Server mit installierter Avira Exchange Security administriert werden als auch ganze "Avira Exchange Security Serverfarmen". Dies erleichtert speziell in einer Multi-Server-Umgebung die tägliche Administration.

Mit der Avira Exchange Security Management Console erhält der Administrator Zugriff auf alle erforderlichen Konfigurationsinformationen und den Avira Monitor (enthält u.a. einen Überblick über die Quarantänen) der Avira Exchange Security Server.

Verwandte Themen:

Starten der Avira Exchange Security Management Console - Seite 5

Konfiguration in der Avira Exchange Security Management Console - Seite 6

3.1.1 Zugriffsmethoden

Für die Konfiguration und die Zugriffe auf die Quarantänen werden zwei unterschiedliche Zugriffsmethoden verwendet.

1. Standard Windows Dateizugriff

   Für den Zugriff auf die Avira Exchange Security Konfiguration, um beispielsweise Sicherheitseinstellungen zu administrieren, ist ein Windows Dateizugriff erforderlich. Hierbei kann die Avira Exchange Security Konfiguration lokal zur Verfügung stehen.
2. SOAP und SSL

   Der Zugriff auf den Avira Monitor erfolgt über SOAP und SSL. Dabei wird über einen festgelegten Kommunikationsport kommuniziert.

Verwandte Themen:

Avira Monitor - Seite 22

3.1.2 Betriebsmodi

Die Avira Exchange Security Management Console unterstützt zwei Betriebsmodi.

1. Lokale Administration

Die Avira Exchange Security Management Console wird direkt auf dem Exchange-Server betrieben, auf welchem alle Avira Exchange Security-Komponenten installiert wurden. Dieser Modus eignet sich für kleinere Umgebungen und die Administration am Server vor Ort.

2. Remote Administration

   Die Avira Exchange Security Management Console wird nicht auf dem Exchange-Server, sondern auf einem Client installiert.

Die Remote Administration eignet sich für die zentrale Administration in Multi-Server-Umgebungen. Die Avira Exchange Security Management Console greift dabei auf einen oder mehrere Exchange-Server zu, um die Avira Exchange Security zu konfigurieren und zu administrieren.

3.2 Avira Exchange Security Server

Mit Avira Exchange Security Server werden die Funktionen und Prozesse von Avira Exchange Security bezeichnet, die ausschließlich auf dem Exchange-Server laufen.

Der Avira Exchange Security Server kann sowohl in einfachen Umgebungen als auch in Front-End/Back-End-Umgebungen installiert werden.

Der Avira Exchange Security Server unterteilt sich wiederum in verschiedene Bereiche.

3.2.1 Der Transport-Agent

Der Transport-Agent ist ein Prozess, der dafür zuständig ist, dass alle Emails, Terminanfragen, etc., die der Exchange-Server versendet, empfängt oder routet, "abgegriffen" (Englisch: to grab) werden.

Für den gesamten Transport von Emails, Terminanfragen, etc. wird das SMTP-Transportprotokoll verwendet. Ein Bestandteil des SMTP-Transportprotokolls ist der "Microsoft SMTP Transportstapel" (Englisch: "MS SMTP Transport Stack"). Durch diesen Transport Stack wird der komplette Email-Verkehr geleitet. Dabei ist es unerheblich, ob es sich um Emails handelt, die zwischen Postfächern auf dem gleichen Postfachspeicher oder Server gesendet werden oder um ein- und ausgehende Emails.

In allen Fällen müssen Emails den Transport Stack durchlaufen. Der Transport-Agent ist in diesem Transportstapel "eingeklinkt". Als registrierte Ereignissenke (Englisch: event synk) überwacht der Transport-Agent dort den Email-Verkehr und leitet alle relevanten Informationen an den Avira Exchange Security Dienst – die zweite Komponente des Avira Exchange Security – weiter. Die Email wird so lange aufgehalten, bis die gesamte Verarbeitung durch den Avira Exchange Security Server erfolgreich beendet ist.

Hinweis
Exchange-interne Informationen, wie beispielsweise Replikationsnachrichten, werden vom Transport-Agenten als solche erkannt und unverändert im Exchange-System belassen.

3.2.2 Der Avira Exchange Security Dienst = Enterprise Message Handler (EMH)

Der Avira Exchange Security Dienst ist als Windows Dienst permanent gestartet und übernimmt alle Informationen vom Transport Agent. Die gesamte Weiterverarbeitung durch Avira Exchange Security wird ab diesem Zeitpunkt vom Avira Exchange Security Service überwacht und gesteuert.

Warnung
Wird der Avira Exchange Security Dienst gestoppt, werden die Sicherheitsfunktionen von Avira Exchange Security abgeschaltet.

Der Avira Exchange Security Dienst hat Zugriff auf alle notwendigen Informationen:

- Die konfigurierten Avira Exchange Security Jobs
- Die installierte Avira Exchange Security Lizenz
- Das Active Directory
- Die Avira Exchange Security Quarantäne

Mithilfe all dieser Informationen werden die Emails nun beispielsweise nach Viren überprüft, unerwünschte Emails identifiziert und unter Quarantäne gestellt.

Nach der Bearbeitung übergibt der Avira Exchange Security Dienst die Emails wieder an den SMTP-Server.

3.2.3 Quarantäne

Als eine mögliche Option von Avira Exchange Security können virenverseuchte Emails oder andere unerwünschte Emails auf dem Server gestoppt werden. Damit wird verhindert, dass diese Emails bei den entsprechenden Empfängern ankommen. Die verseuchten Emails werden stattdessen in der Quarantäne abgelegt.

Auf jedem Avira Exchange Security Server stehen nach der Installation einige Quarantänen zur Verfügung. Weitere Quarantänen können vom Administrator angelegt werden.

Eine Quarantäne besteht aus:

- Einem Quarantäneverzeichnis auf dem Exchange-Server (...*Avira**Avira Exchange Security* *AppData**Quarantine**Default Quarantine*).
- Den Emails, die in die Quarantäne kopiert wurden.
- Einer Quarantäne Datenbank (*LocIdxDB.mdb*).

Avira Exchange Security erzeugt für jede unter Quarantäne gestellte Email automatisch einen Eintrag in der Quarantänedatenbank. Bei dieser Datenbank handelt es sich um eine Microsoft Access Datei.

Beim Anzeigen einer Quarantäne mit der Quarantäne werden zunächst die Informationen aus der Quarantänedatenbank angezeigt.

Gespeicherte Informationen in der Quarantäne-Datenbank

In der Quarantäne-Datenbank werden folgende Informationen abgelegt.

- Email-Betreff

- Datum/ Uhrzeit
- Email-Adresse des Absenders
- Email-Adresse des Empfängers
- Email-Adresse des Absenders (SMTP)
- Email-Adresse des Empfängers (SMTP)
- Kurzbeschreibung der entdeckten Restriktion
- Größe der Email
- Name des Avira Exchange Security-Jobs, der die Email unter Quarantäne gestellt hat
- Name des Exchange-Servers
- Name der Email-Datei
- Bearbeitungshistorie

Kommunikation mit der Quarantäne

Die Kommunikation mit der Quarantäne erfolgt mit Hilfe von SOAP (Simple Object Access Protocol) + SSL (Secure Socket Layer). Dies gilt sowohl für den "lokalen" Zugriff auf dem Server direkt als auch für den Zugriff von einer entfernten Windows-Workstation.

Für die Kommunikation wird standardmäßig der Port 8008 verwendet. Dieser Port kann in der Avira Exchange Security Management Console (Server-Knoten) geändert werden. Wird dieser Port für den Server geändert, so muss diese Änderung auch auf allen zugreifenden Konsolen angepasst werden. Alle Rechner müssen den gleichen Port verwenden.

Mit Hilfe von SSL wird der SOAP Kommunikationskanal verschlüsselt. Während der Installation werden hierfür alle notwendigen Komponenten bereitgestellt.

3.2.4 Das Active Directory/LDIF

Avira Exchange Security nimmt keine Veränderungen oder Erweiterungen im Active Directory(AD) vor. Informationen aus dem Active Directory werden jedoch an verschiedenen Stellen von Avira Exchange Security ausgelesen.

Beim Starten ermittelt der Avira Exchange Security Dienst den verfügbaren Global Catalog Server. Dieser wird zum Beispiel bei der Adressauflösung von Verteilerlisten während der Email-Verarbeitung verwendet.

Die Avira Exchange Security Management Console verwendet das Active Directory bei der Auswahl von Sender/Empfänger Bedingungen.

Steht kein Active Directory zur Verfügung, da z. B. die entsprechenden Ports nicht offen sind, kann mit einer LDIF-Datei gearbeitet werden. Diese kann beispielsweise durch einen LDAP-Export aus einem Active Directory, Exchange Benutzerverzeichnis oder einem Notes Name- and Addressbook (Namens- und Adressbuch - NAB) erzeugt werden.

3.2.5 Komprimierte Dateien/Archive - Avira Exchange Security Unpacker

Wenn Dateien per Email verschickt werden, geschieht dies häufig in komprimierter Form. Damit der Virenscan und alle Prüfungen auch bei Archiven funktionieren, beinhaltet Avira Exchange Security einen Entpacker, um auch Dateien in Archiven prüfen zu können.

Der Entpacker unterstützt die folgenden Archivformate:

- ACE
- CAB
- ZIP
- Selbstentpackendes ZIP
- ARJ
- Selbstenpackendes ARJ
- TAR
- GZIP
- TGZ (Bandarchive)
- UUE (komprimierte ausführbare ASCII Archive)
- LZH (LH ARC)
- RAR
- Selbstentpackendes RAR
- Java Archive (*.jar)
- BZIP 2
- 7-ZIP

Hinweis
Innerhalb eines Archivs können sich wiederum Archive befinden. Diese Archive (rekursiv gepackte Dateien) werden standardmäßig bis zu einer Entpackungstiefe von 5 entpackt. Alle Archive, die dieses Limit überschreiten, werden in den BADMAIL-Bereich überführt.

Die Standard-Obergrenze für eine Email inkl. entpackter Dateien beträgt 300 MB. Insbesondere bei so genannten "ZIP of Death"-Attacken ist eine solche Begrenzung wichtig. Die Entpackungstiefe und die Größenlimitierung können in der Konsole unter **Basiskonfiguration** › **Avira Server** › **Eigenschaften** › **Allgemein** geändert werden.

3.3 Die Konfigurationsdatei von Avira Exchange Security

Alle Informationen, die zum Betreiben von Avira Exchange Security erforderlich sind, werden als XML-Datei (*ConfigData.xml*) mit separaten Einträgen für jeden Konfigurationsbereich in der Konfiguration gespeichert.

Da es sich bei der Konfiguration um eine einzelne Datei handelt, ist es sehr einfach, die Konfiguration zu verteilen und zu sichern. Für Unterstützung bei Konfigurationsproblemen kann die *ConfigData.xml* zur Analyse an das Avira Support Team gesendet werden.

Die Konfigurationsdaten werden sowohl vom Avira Exchange Security Server als auch von der Avira Exchange Security Management Console benötigt. Der Avira Exchange Security Server verwendet z. B. diese Daten für den Avira Exchange Security Job.

Um mit der Avira Exchange Security Management Console Änderungen an der Konfiguration vornehmen zu können, benötigt auch sie Zugriff auf die Datei *ConfigData.xml*.

Die Konfigurationsdaten für Avira Exchange Security können sowohl in einem lokalen Verzeichnis als auch auf einem Netzwerkshare gespeichert werden. Welche Konfiguration von Avira Exchange Security die Avira Exchange Security Management Console bzw. der Avira Exchange Security Server verwendet, wird durch einen Eintrag in der Registry festgelegt.

Der Pfad zur Avira Exchange Security Konfiguration kann im Format "C:\..." oder als UNC-Pfad *Servername**Share**ConfigData.xml* angegeben werden.

Wenn die angegebene Avira Exchange Security Konfiguration nicht verfügbar ist, verwendet Avira Exchange Security die letzte als funktionierend bekannte Konfiguration, die in der Ereignisliste von Windows protokolliert ist.

Die letzte als funktionierend bekannte Konfiguration wird für jeden Server lokal gespeichert und stets aktualisiert, wenn Änderungen an der Avira Exchange Security Konfiguration vorgenommen werden. Über die Avira Exchange Security Konfiguration kann auf die letzte als funktionierend bekannte Konfiguration zugegriffen werden.

3.3.1 Verwendung einer benutzerdefinierten Konfigurationsdatei

Um eine benutzerdefinierte Konfigurationsdatei verwenden zu können, steht ein Parameter zur Verfügung.

Um eine benutzerdefinierte Konfigurationsdatei in der Konsole öffnen zu können, starten Sie die Datei *Avira.msc* mit dem Parameter `config` und der erforderlichen Konfigurationsdatei.

```
"C:\Programme(x86)\Avira\Avira Exchange Security\Avira.msc"
 config "C:\Anderer Ordner\Verzeichnis\ConfigData.xml"
```

Sie können hier auch einen UNC-Pfad angeben.

4 Avira Monitor

Im Avira Monitor können Sie alle Quarantänen und Bad-Mails auf allen verfügbaren Servern beobachten. Außerdem haben Sie hier Zugriff auf die Statistik-Auswertungen.

Im Avira Monitor sind alle Server gelistet, die unter **Basiskonfiguration** › **Avira Server** konfiguriert sind.

Der Avira Monitor greift mit SOAP/SSL-Verschlüsselung über das Netzwerk auf die Server zu.

Verwandte Themen:

Zugriffsmethoden - Seite 16

4.1 Zugriff auf den Avira Monitor einrichten

1. Um auf einen Server zugreifen zu können, tragen Sie ihn zunächst unter **Basiskonfiguration** › **Avira Server** ein und aktualisieren den Avira Monitor in der Ansicht.

Hinweis
Der Zugriff auf Details im Avira Monitor hängt außerdem von der Konfiguration jeder Quarantäne ab.

2. Um sich umfassende Informationen über die Avira Exchange Security Version und die Konfiguration anzeigen zu lassen, klicken Sie im **Avira Monitor** mit der rechten Maustaste den gewünschten Server und wählen Sie **Eigenschaften**.
3. Sollten Sie nicht lokal auf dem Server angemeldet sein, erscheint ein Anmeldedialog, in dem Sie Ihren Benutzernamen und das Passwort für die entsprechende Domäne eingeben. Die Berechtigung für den Avira Monitor-Zugriff wird in den Eigenschaften der Datei *access.acl* im Ordner ...*Avira**Avira Exchange Security**AppData* eingetragen.
4. Klicken Sie die Registerkarte **Sicherheit** und geben Sie den gewünschten Benutzern mindestens einen Lesezugriff.

Verwandte Themen:

Einstellungen für einen individuellen Avira Server - Seite 111
Konfiguration der Quarantäne - Seite 139

4.2 Verwendung des Avira Monitor

1. Klicken Sie den gewünschten Server.
2. Authentifizieren Sie sich mit einem Benutzernamen und Passwort, der auf dem Dateisystem des Servers Berechtigungen für die Avira Daten besitzt.
3. Klicken Sie in den Bereich, den Sie einsehen wollen, also beispielsweise auf **Standard-Quarantäne** oder **BADMAIL**.
   Alle vorhandenen Emails werden angezeigt (Anzeigegrenze 10.000 Emails).

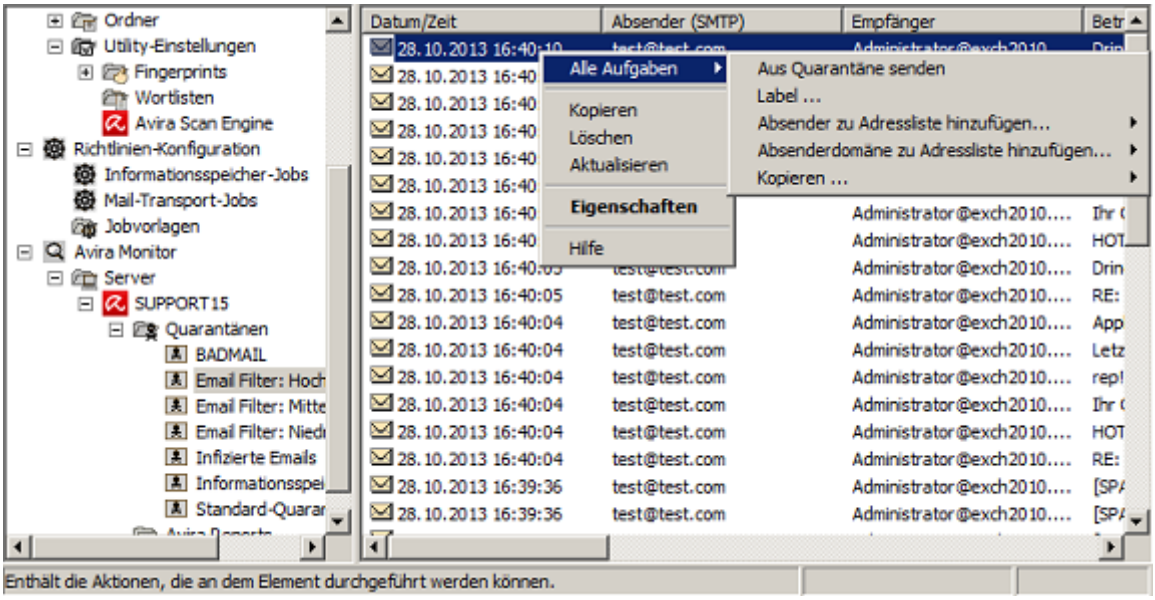
4. Verfügbare Aktionen:
   - Filtern Sie die gewünschten Emails mit dem **Filteroptionen**-Symbol aus.
   - Öffnen Sie eine Email mit einem Doppelklick.
   - Versenden Sie die Email mit einem Klick auf die Schaltfläche bei Bedarf erneut.

4.3 Quarantänen verwenden

Wenn Sie im Job die Aktion **In Quarantäne kopieren** aktiviert haben, befinden sich alle betroffenen Emails in einer Quarantäne und Sie erhalten im Avira Monitor alle verfügbaren Informationen über die einzelnen Emails.

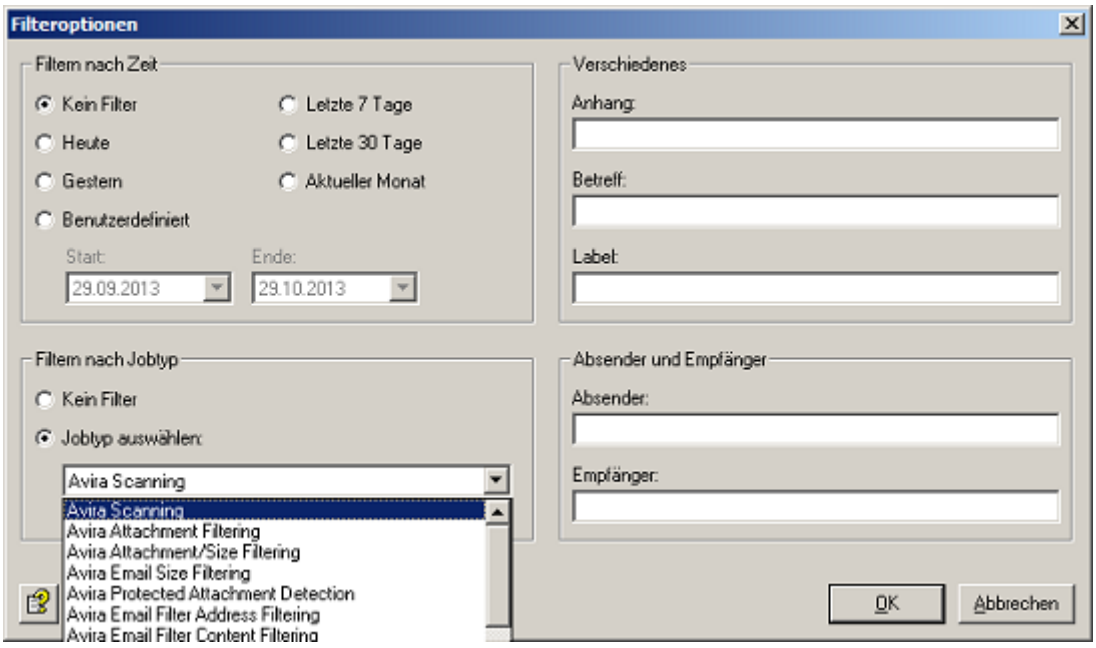
Innerhalb einer Quarantäne ist es möglich, die Emails nach zahlreichen Auswahlkriterien zu filtern.

1. Klicken Sie auf eine Quarantäne.
   In der Ansicht im Avira Monitor werden maximal 10.000 Emails auf einmal angezeigt (die neuesten).
2. Verfügbare Aktionen:
   - Ältere Emails, die nicht mehr mit aufgeführt werden, erhalten Sie durch Einschränken der Ansicht mit einer entsprechenden Filteroption.
   - Wenn Sie eine Email in eine andere Quarantäne kopieren möchten, ziehen Sie diese per Drag-and-Drop in die Ziel-Quarantäne.
   - Klicken Sie mit der rechten Maustaste auf die Email in der Liste und wählen Sie eine Aktion aus.



3. Emails filtern:

- Klicken Sie mit der rechten Maustaste **Ansicht** › **Filteroptionen**.
- Klicken Sie das **Filteroptionen**-Symbol .

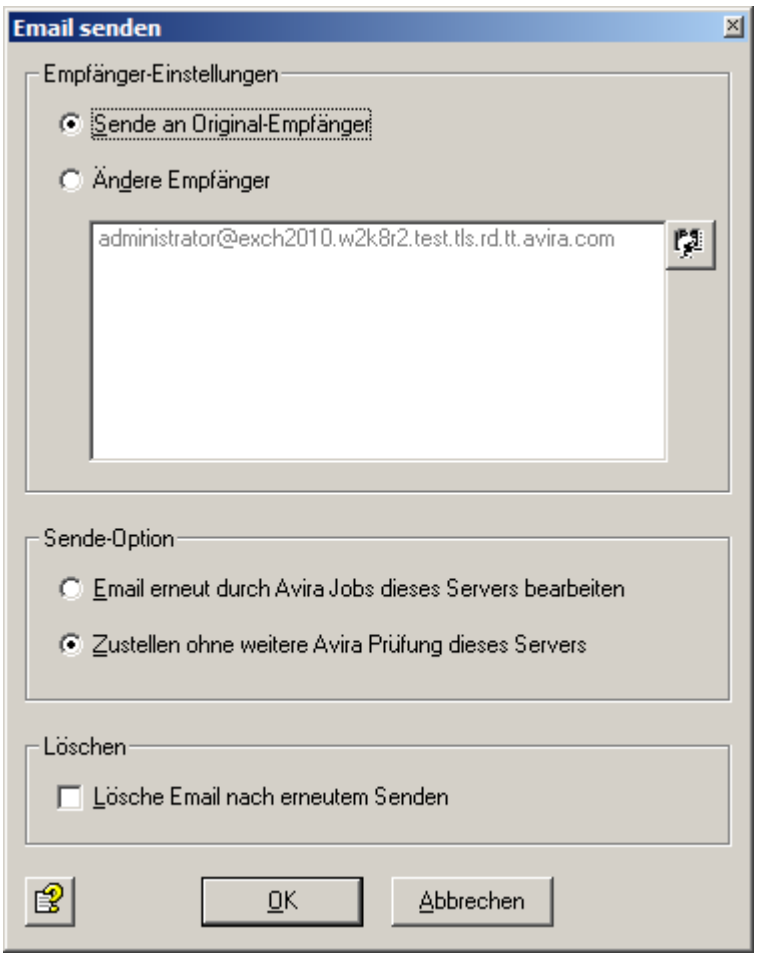


4. Filter zurücksetzen:
   - Aktivieren Sie die Option **Kein Filter** in **Filteroptionen**.
   - Klicken Sie mit der rechten Maustaste auf **Ansicht** › **Alle Objekte anzeigen**.
   - Benutzen Sie das Symbol **Filter deaktivieren** in der Symbolleiste.

4.4 Emails aus der Quarantäne senden

Wenn Sie eine Email aus der Quarantäne wieder seinem ursprünglichen oder einem weiteren Empfänger zukommen lassen möchten, können Sie diese direkt aus der Quarantäne versenden, ohne dass sie erneut von einem Avira Exchange Security Job geprüft wird.

1. Öffnen Sie eine Liste von Emails einer Quarantäne im **Avira Monitor**.
2.
   - Wählen Sie die erwünschte Email mit der rechten Maustaste aus und aktivieren Sie nun **Alle Aufgaben** › **Aus Quarantäne senden**.
   - Aktivieren Sie die **Sende an Original-Empfänger** Option im **Eigenschaften**-Fenster.



Der Empfänger sieht im **Von**-Feld den Original-Absender der Email (keine Weiterleitungsemail).

3. Optional: Sie können den Empfänger ändern, indem Sie die Option **Ändere Empfänger** aktivieren und dann auf die Schaltfläche **Adresse auswählen** klicken.

Hinweis
Bei der Auswahl der Adressen für das erneute Versenden aus der Quarantäne stehen keine Adresslisten zur Verfügung.

4. Wenn Sie die Email nicht mehr durch die Jobs bearbeiten lassen möchten, so aktivieren Sie die Option **Zustellen ohne weitere Avira Prüfung dieses Servers**.

   Das wird der Regelfall sein, wenn Sie eine Email aus der Quarantäne wieder zustellen lassen, weil ein Benutzer diese Email trotz z.B. verbotener Wörter oder Anhängen dringend braucht.

Hinweis
Es handelt sich hier um eine übergreifende Einstellung. Sollten Sie Jobs aktiviert haben, die auch erneut gesendete Emails aus der Quarantäne prüfen sollen, so setzen Sie diese Einstellung auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**, ansonsten greift die Jobeinstellung **Vor Versand prüfen** nicht und es werden alle Emails unbearbeitet weitergesendet.

Hinweis
Die Anweisung **Email erneut durch Avira Jobs dieses Servers bearbeiten** gilt auch nur für diejenigen Jobs, bei denen die Option **Emails aus Quarantäne: Vor Versand prüfen** aktiviert

worden ist. Selbst wenn Sie also die Quarantäne-Emails erneut bearbeiten lassen wollen, werden alle Jobs ausgeklammert, bei denen **Ohne Prüfung versenden** aktiviert ist.

Verwandte Themen:
Adresslisten - Seite 124

4.5 Absender einer Adressliste hinzufügen

Die Option **Adressen dürfen aus Quarantäne hinzugefügt werden** muss für die Adressliste aktiviert sein. Anderenfalls kann die gewünschte Absenderadresse nicht der Liste hinzugefügt werden.

Wenn die Email eines Absenders unter Quarantäne gestellt wurde, dessen Emails aber zukünftig als erwünscht erkannt werden sollen, können Sie den Absender auf eine Ihrer Adresslisten setzen, z. B. *Email Filter: Whitelist*.

1. Öffnen Sie im **Avira Monitor** die Quarantäne, die die erwünschte Email enthält.
2. Wählen Sie die Email mit der rechten Maustaste aus und aktivieren Sie nun **Alle Aufgaben** › **Aus Quarantäne senden**.
3. Wählen Sie die Adressliste, in die der Absender aufgenommen werden soll.

Verwandte Themen:
Adresslisten - Seite 124

4.6 Domain einer Adressliste hinzufügen

Die Option **Adressen dürfen aus Quarantäne hinzugefügt werden** muss für die Adressliste aktiviert sein. Anderenfalls kann die gewünschte Absenderdomain der Liste nicht hinzugefügt werden.

Wenn Emails von einer bestimmten Domain unter Quarantäne gestellt wurden, die Emails aller Benutzer von dieser Domain aber zukünftig als erwünscht erkannt werden sollen, können Sie die Domain auf eine Ihrer Adresslisten setzen.

Sie müssen dafür nicht alle Absenderadressen einzeln in die Adressliste eintragen. Die Adresse kann der Liste in der Form `*@beispielunternehmen.de` hinzugefügt werden.

1. Öffnen Sie im **Avira Monitor** die Quarantäne, die die erwünschte Email enthält.
2. Wählen Sie die Email mit der rechten Maustaste aus und aktivieren Sie nun **Alle Aufgaben** › **Absenderdomäne zu Adressliste hinzufügen**.
3. Wählen Sie die Adressliste, in die der Absender aufgenommen werden soll.

4.7 BADMAIL

BADMAIL sind alle Emails, die durch die Avira-Jobs nicht bearbeitet werden konnten, wie beispielsweise Emails mit nicht verarbeitbaren Formaten.

Über Bad-Mails existieren sehr wenig Informationen, da Avira keine Einsicht in diese Emails nehmen konnte. Diese Emails können also auch einen unentdeckten Virus enthalten.

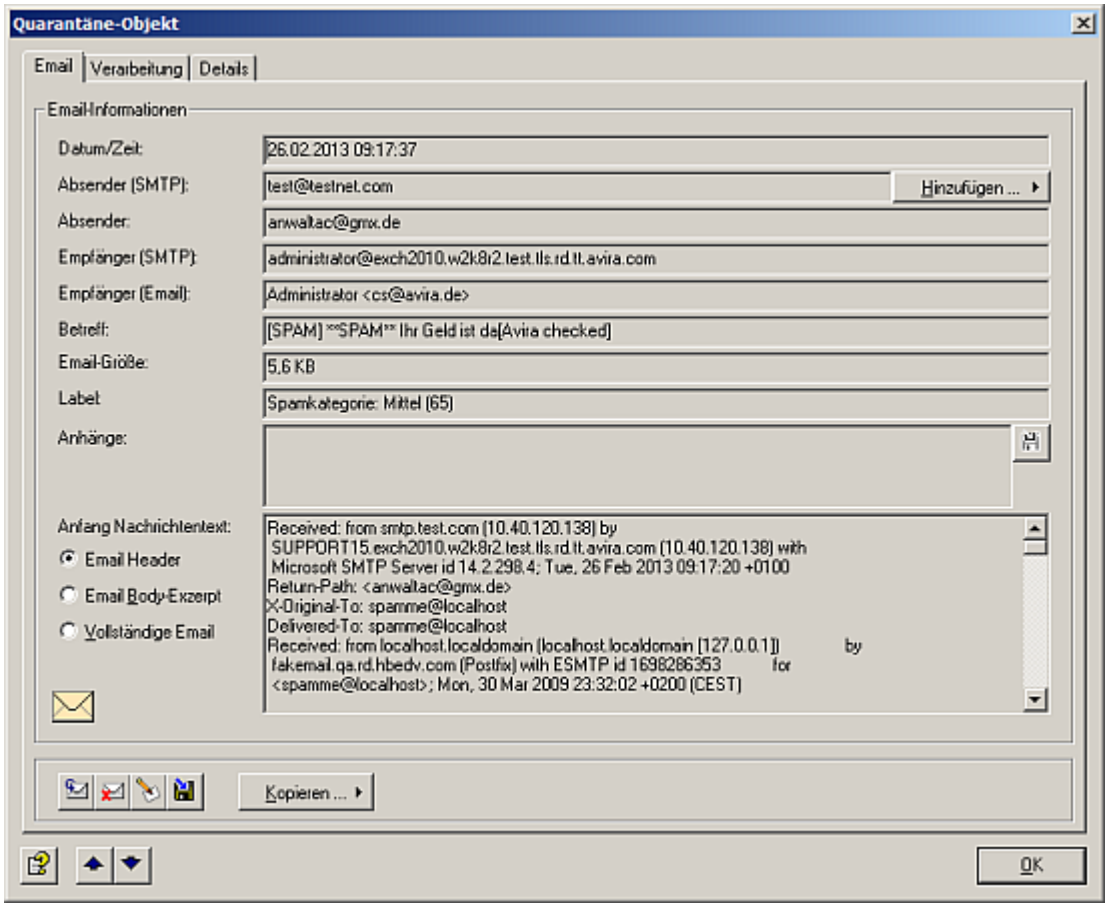
Für Bad-Mails existiert auf jedem Server nur ein Ordner. Es können auch keine weiteren Ordner angelegt werden. Ansonsten gelten für Bad-Mails die gleichen Funktionen und Optionen wie für Quarantäne-Mails.

4.8 Details einer unter Quarantäne gestellten Email

Sie erhalten Details über eine unter Quarantäne gestellte Email, wenn Sie mit einem Doppelklick oder der rechten Maustaste die Eigenschaften der Email in der Quarantäne-Liste aufrufen.

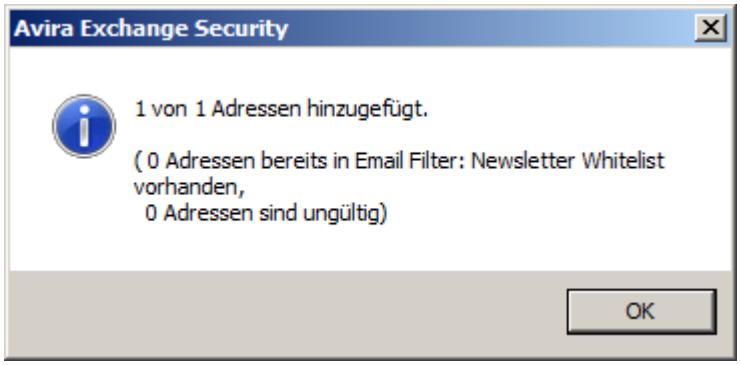
4.8.1 Email-Details

Unter der Registerkarte **Email** finden Sie das Wichtigste auf einen Blick.



Die Schaltfläche **Hinzufügen** ermöglicht es, den SMTP-Absender der Email zur Abwehr einer bestimmten Adressliste hinzuzufügen. Welche Adresslisten unter dieser Schaltfläche angezeigt werden, definieren Sie für jede einzelne Adressliste.

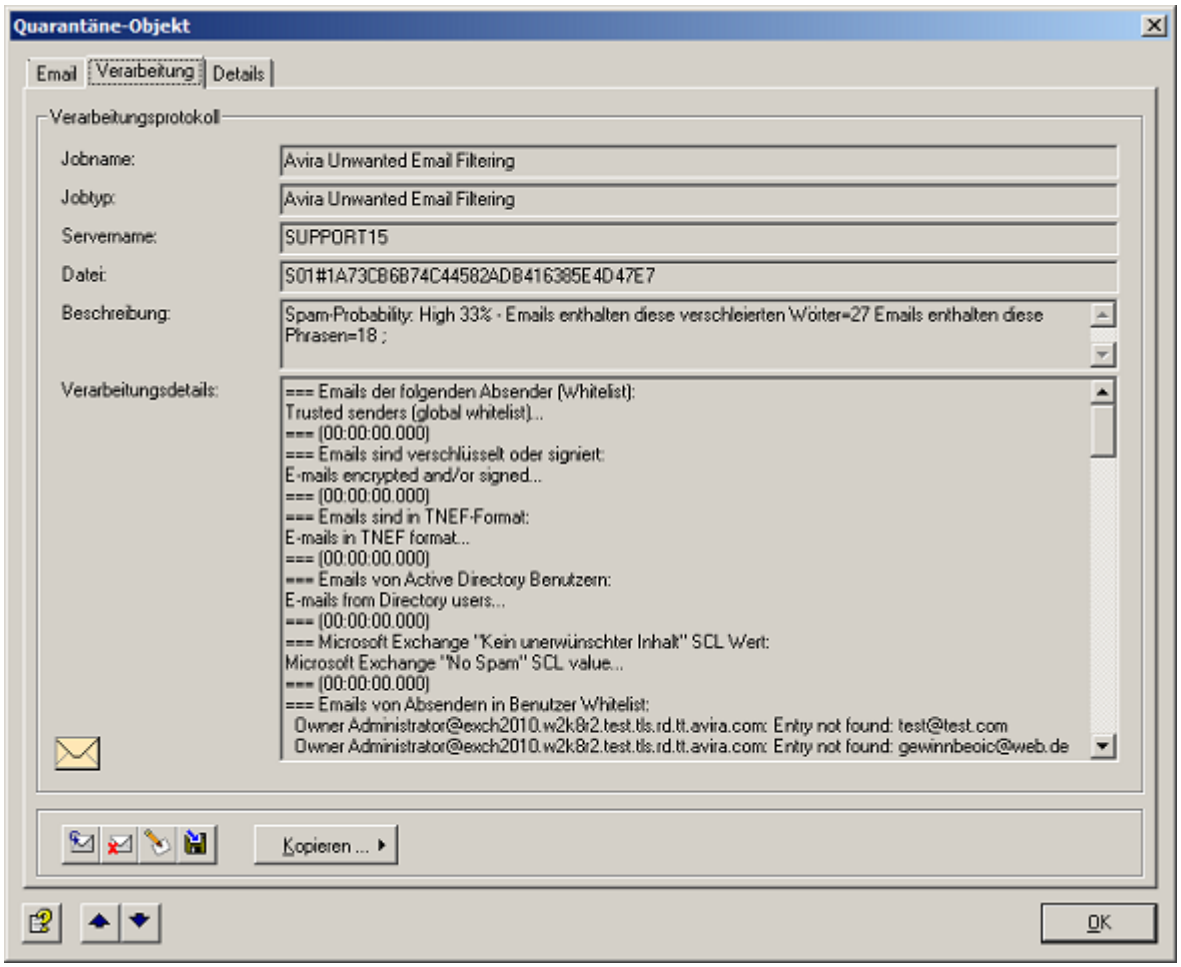
Sobald die Absenderadresse der Adressliste hinzugefügt worden ist, erhalten Sie eine Meldung.


Avira Exchange Security
1 von 1 Adressen hinzugefügt.
(0 Adressen bereits in Email Filter: Newsletter Whitelist vorhanden,
0 Adressen sind ungültig)
OK

Verwandte Themen:
Adresslisten - Seite 124

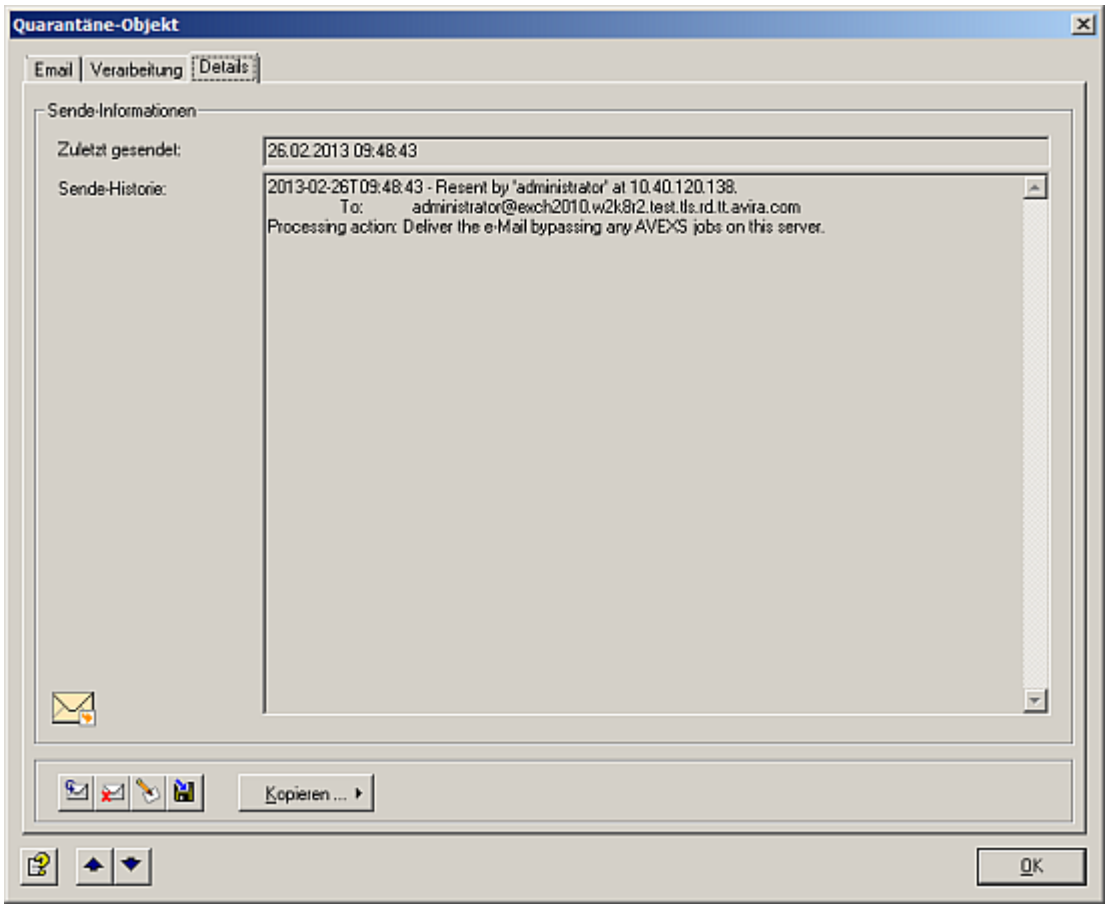
4.8.2 Quarantäne-Verarbeitungsprotokoll

Der Name des Jobs, der die Email unter Quarantäne gestellt hat, Art des Jobs, der Server, der Grund, aus dem die Email blockiert und unter Quarantäne gestellt wurde sowie weitere Details zur Verarbeitung können unter **Verarbeitung** abgerufen werden.



4.8.3 Quarantäne-Details

Unter **Details** erhalten Sie den Verlauf des erneuten Sendens aus der Quarantäne.

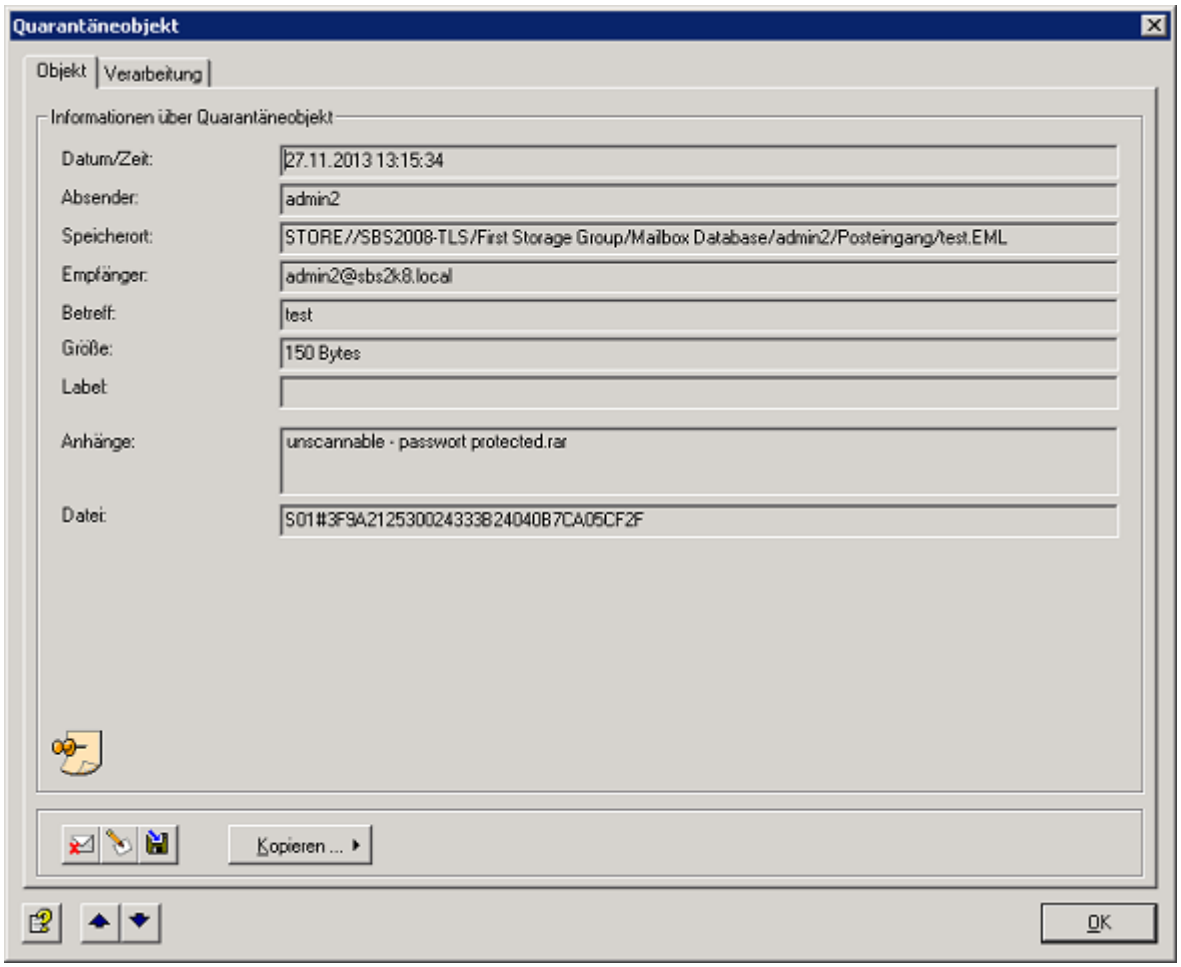


4.9 Details in der IS-Quarantäne

Sie erhalten Details über eine unter Quarantäne gestellte Email, wenn Sie mit einem Doppelklick oder der rechten Maustaste die Eigenschaften der Email in der Quarantäne-Liste aufrufen.

4.9.1 Email-Details in der IS-Quarantäne

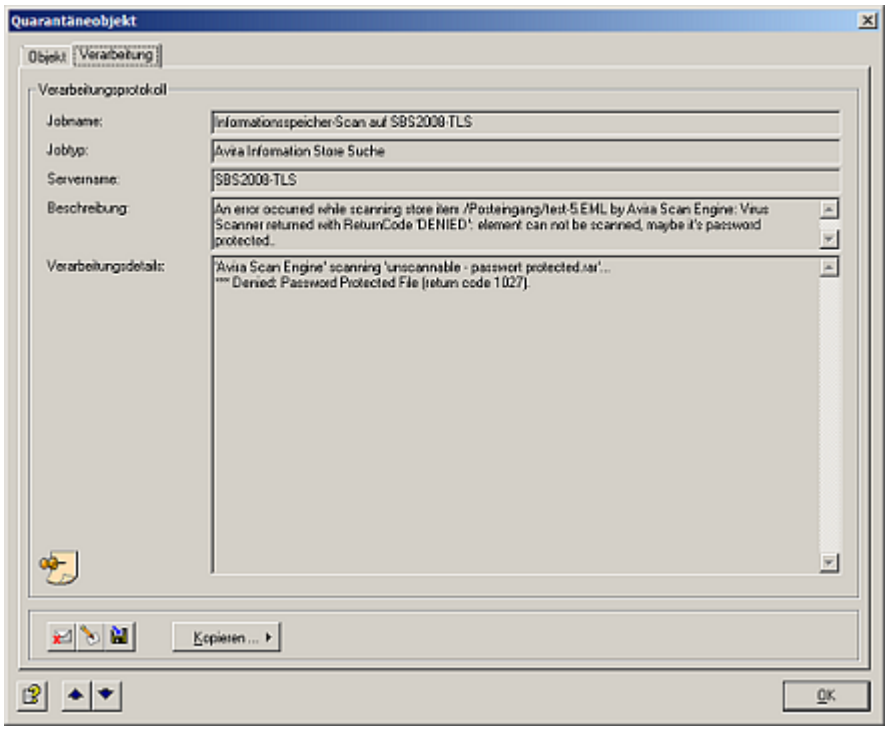
Unter der Registerkarte **Objekt** finden Sie auf einen Blick das Wichtigste über die Emails in der Informationsspeicher-Quarantäne.



Die Schaltfläche **Kopieren** ermöglicht es, das Objekt in eine andere, auf diesem Server vorhandene, Quarantäne zu kopieren.

4.9.2 IS Quarantäne-Verarbeitungsprotokoll

Der Name des Jobs, der die Email unter Quarantäne gestellt hat, Art des Jobs, der Server, der Grund, aus dem die Email blockiert und unter Quarantäne gestellt wurde sowie weitere Details zur Verarbeitung können unter **Verarbeitungsprotokoll** abgerufen werden.



4.10 Quarantäne-Schaltflächen

Liste der für die Quarantäne verfügbaren Schaltflächen

Schaltfläche	Aktion
	Email aus Quarantäne (nicht der IS-Quarantäne) senden
	Email in Quarantäne löschen
	Label für die Email festlegen, ändern, löschen
	Email speichern unter
	Online-Hilfe öffnen
	Nächste Email in der Quarantäne/Badmail
	Vorherige Email in der Quarantäne/Badmail

4.11 Avira Exchange Security-Statistiken

Mithilfe der **Avira Monitor**-Funktion von Avira Exchange Security können detaillierte Informationen über die Email-Verarbeitung abgerufen werden.

Es stehen verschiedene vordefinierte und ein erweiterter Statistik-Report zur Verfügung. Der erweiterte Statistik-Report kann individuell definiert werden. Die einzelnen Reports enthalten sowohl grafische Darstellungen von erkannten Richtlinienverletzungen (z.B. Viren, unerwünschte Dateianhänge) als auch tabellarische Informationen. Zu den gängigsten Fragestellungen steht ein eigener Report bereit. Darüber hinaus werden Daten zu Avira Quarantänen dargestellt.

Die Statistiken können für frei definierbare Zeiträume erstellt werden.

Die Druck- und Export-Schaltflächen ermöglichen die einfache Weiterverwendung der Statistik-Daten.

Bearbeitete Emails erscheinen grundsätzlich nicht sofort in den Statistiken. Die Report-Daten werden während der Verarbeitung zwischengespeichert und zwei Mal pro Stunde in die Auswertungsdatenbank geschrieben.

4.12 Erstellung von Statistiken

1. Klicken Sie **Avira Berichte**.
2. Doppelklicken Sie in der Statistiken-Liste auf den Namen der Statistik, die Sie erstellen wollen.
3. Geben Sie den gewünschten Zeitrahmen für die Datenerfassung ein.
4. Um die Daten zu exportieren, klicken Sie die Schaltfläche **Exportieren** .
   Sie können zwischen unterschiedlichen Formaten wählen.

5 Avira Scan Engine

Mit Avira Scan Engine überprüfen Sie die Emails auf Viren, auf Typ und Größe eines Anhangs und auf die Gesamt-Email-Größe.

Hinweis
Legen Sie für jeden Einschränkungstyp einen separaten Job an. Die Jobarten lassen sich später nicht mehr ändern.

Jobarten

Jobart	Beschreibung
Avira Prüfung	Virenprüfung ein- und ausgehender Emails
Suche im Informationsspeicher	Virenprüfung der MS Exchange Datenbanken (in Echtzeit & proaktiv/im Hintergrund)
Avira geschützte Anhangserkennung	Blockieren passwortgeschützter Archive
Avira Anhangsfilterung	Sperren von bestimmten Dateitypen im Anhang
Avira Email-Größenfilterung	Beschränkung der Email-Größe
Avira Anhangs-/Größenfilterung	Beschränkung von Typ und/oder Größe der Anhänge

5.1 Avira Prüfung-Jobs

Den Virenscanner können Sie unter **Basiskonfiguration** > **Utility-Einstellungen** > **Avira Scan Engine** > **Eigenschaften** konfigurieren.

Der Avira Prüfung Job startet gemäß den konfigurierten Bedingungen den Virenscanner. Die Bedingungen bestimmen, für welche Emails ein Job ausgeführt wird.

Folgendes Beispiel illustriert die Vorgehensweise eines Jobs für die Virenprüfung: Der Job prüft eine Email mit dem Ergebnis *Virus gefunden*. Daraufhin wird Virenalarm ausgelöst und eine Reihe von Aktionen in Gang gesetzt, die Sie selbst unter Aktionen definieren können.

Weitere Szenarien sind möglich:

- Wenn ein Virus gefunden wird, soll die Original-Email repariert und dann dem Empfänger zugestellt werden.
- Wenn die Original-Email nicht gereinigt werden kann, wird die betroffene Email in den von Ihnen gewählten Ordner (Quarantäne) kopiert, das Original gelöscht und nicht zugestellt.
- In diesem Fall werden Nachrichten an Administrator, Absender und Empfänger gesendet, die die relevanten Informationen des Virenscanners und Avira Prüfung Job enthalten.

Diese Aktionen sind möglich:

- Auf Viren prüfen
- Von Viren reinigen
- Zusatz im Betreff
- Gesamte Email in Quarantäne kopieren
- Betroffene Anhänge aus Email entfernen
- Betroffene Email löschen und nicht zustellen
- Ausführen einer externen Anwendung
- Administrator, Absender, und/oder Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Header Feld und Wert hinzufügen
- Email umleiten
- Avira Tag und Wert hinzufügen
- Header entfernen

5.1.1 Avira Scan Engine konfigurieren und aktivieren

Unter **Basiskonfiguration** > **Utility-Einstellungen** > **Avira Scan Engine** > **Eigenschaften** können Sie Avira Scan Engine konfigurieren.

Aus der Registerkarte **Jobs** ersehen Sie, in welche Jobs der Virenscanner eingebunden ist.

In der Registerkarte **Returncodes** können Sie die vorkonfigurierten Returncodes bearbeiten. Die Bedeutung der einzelnen Codes finden Sie auf der Registerkarte **Details**.

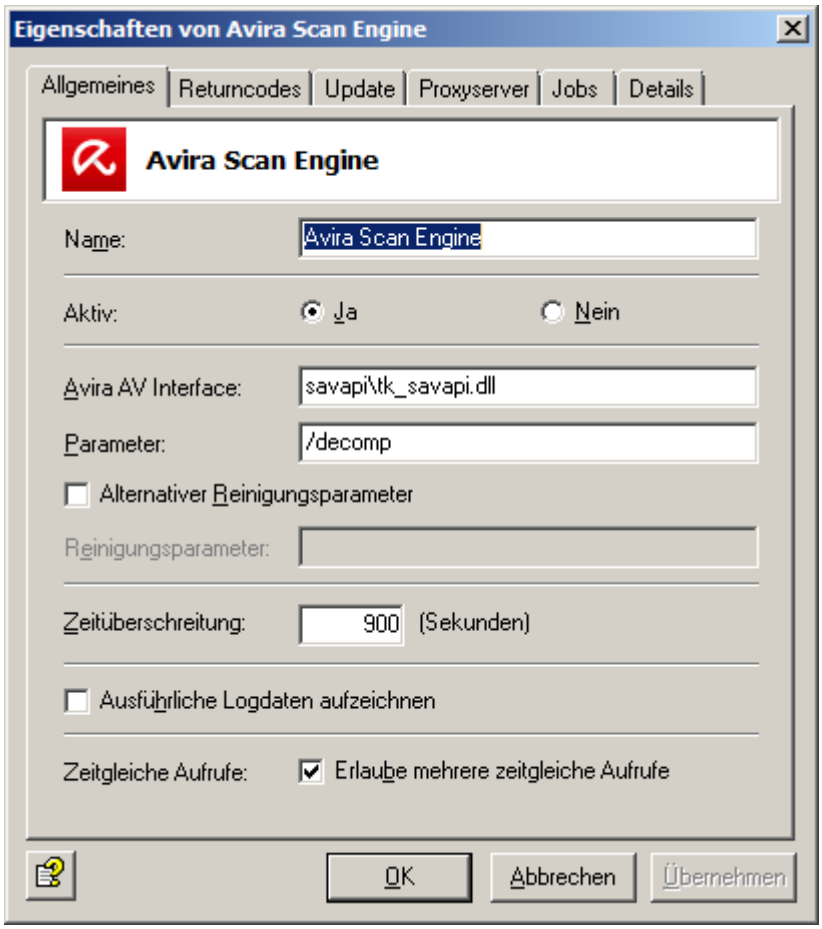
Testen der DLL-Schnittstelle

Avira Exchange Security ruft den Virenscanner durch das sogenannte Avira AV-Oberfläche, eine DLL-Datei, auf.

Warnung
Deaktivieren Sie die Echtzeit- oder On-Access-Scanner verwendeter Virenscanner für das Verzeichnis ...*Avira**Avira Exchange Security**AppData*.

1. Markieren Sie unter Avira Monitor den gewünschten Servernamen und klicken Sie im rechten Fenster auf **Server Status**.
2. Auf der Registerkarte **Suchengine-Test** wählen Sie **Virenscanner-Test**.
   Bei Erfolg erhalten Sie ein *OK* und die Meldung, dass ein EICAR Testvirus gefunden wurde.

Generelle Eigenschaften für Avira Scan Engine



- Im Feld Avira AV-Oberfläche muss der Name der Avira Interface-DLL eingetragen sein. Diese DLL-Datei stellt die Verbindung der Avira Exchange Security zum Virenscanner her. Dieser Eintrag ist für jeden Virenscanner vorkonfiguriert und darf nicht geändert werden.
- Im Folgefeld geben Sie den **Parameter** an, der vom Virenscanner zur Virenprüfung (Scan) verwendet werden soll.
- Um den Virenscanner so einzustellen, dass Emails oder Anhänge bei einem gefundenen Virus bereinigt werden, aktivieren Sie das Feld **Alternativer Reinigungsparameter** und geben im Folgefeld **Reinigungsparameter** den zugehörigen Parameter an.

Hinweis

Die entsprechenden Reinigungsparameter können Sie telefonisch oder per Email beim Avira Support erfragen.

Hinweis

Wenn Sie den Virenscanner nur zur Virenprüfung einsetzen möchten, verwenden Sie den Avira Prüfung-Job. Das Feld **Virus entfernen** muss auf der Registerkarte **Aktionen** deaktiviert sein. Wenn der Virenscanner einen gefundenen Virus auch entfernen soll, verwenden Sie den Job *Prüfung und Entfernung mit Avira Scan Engine*. In diesem Fall müssen das oben genannte Feld **Virus entfernen** aktiviert und die gewünschten Aktionen im Virusfall festgelegt sein.

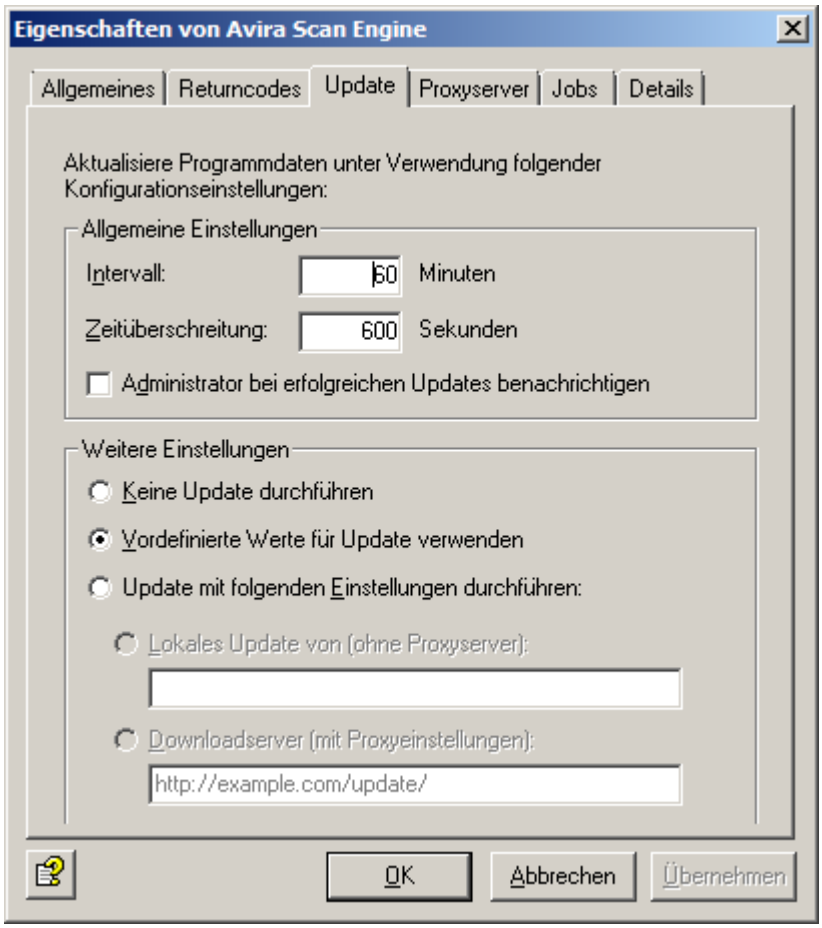
- **Zeitüberschreitung**: Geben Sie die Anzahl der Sekunden an, nach der ein Versuch, die Verbindung zum Server herzustellen, abgebrochen wird (wenn die Verbindung bis dahin noch nicht aufgebaut sein sollte). Berücksichtigen Sie bei der Zeitangabe die Leistungsstärke Ihres Servers. Minimalwert: 60 Sekunden.
- **Erlaube mehrere zeitgleiche Aufrufe**: Legt fest, dass mehrere Emails gleichzeitig durch diesen Virenscanner bearbeitet werden können. Die Anzahl der Aufrufe wird in **Avira Exchange Security Server** › **Eigenschaften** › **Allgemein** › **Anzahl der Threads** definiert. Siehe auch Einstellungen für einen einzelnen Avira Exchange Security Server.

Verwandte Themen:

Einstellungen für einen individuellen Avira Server - Seite 111

Update-Eigenschaften der Avira Scan Engine

Der Virenscanner verfügt über einen Mechanismus, mit dem er die neuesten Erkennungs-Patterns aus dem Internet lädt.



- **Intervall**: Zeitintervall in Minuten, in dem nach der Virenpattern-Aktualisierung gesucht wird. Mindestwert: 15 Minuten.

- **Zeitüberschreitung**: Nach Ablauf dieser Frist wird der Update-Vorgang abgebrochen. Mindestwert: 60 Sekunden.
- **Downloadserver (mit Proxyeinstellungen)**: Sie können für die Aktualisierung der Virenpatterns einen Proxyserver verwenden. Wählen Sie den gewünschten Proxyserver auf der Registerkarte **Proxyserver** aus.

Warnung
Bitte nutzen Sie für Aktualisierungen von Avira Exchange Security nicht diese Registerkarte, sondern wählen Sie unter **Avira Monitor** › **Server-Status** › **Suchengine-Test** die Option **Virenscanner Aktualisierung** und klicken Sie **Start**. Nach dem Update erhalten Sie einen detaillierten Update-Bericht.

5.1.2 Virenprüfung aktivieren

1. Doppelklicken Sie den Job **Prüfen mit der Avira Scan Engine** unter **Richtlinien-Konfiguration** › **Mail-Transport-Jobs**.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.
   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.
4. Adressbedingungen einrichten.
   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.
5. Inhaltliche Bedingungen einrichten.
   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

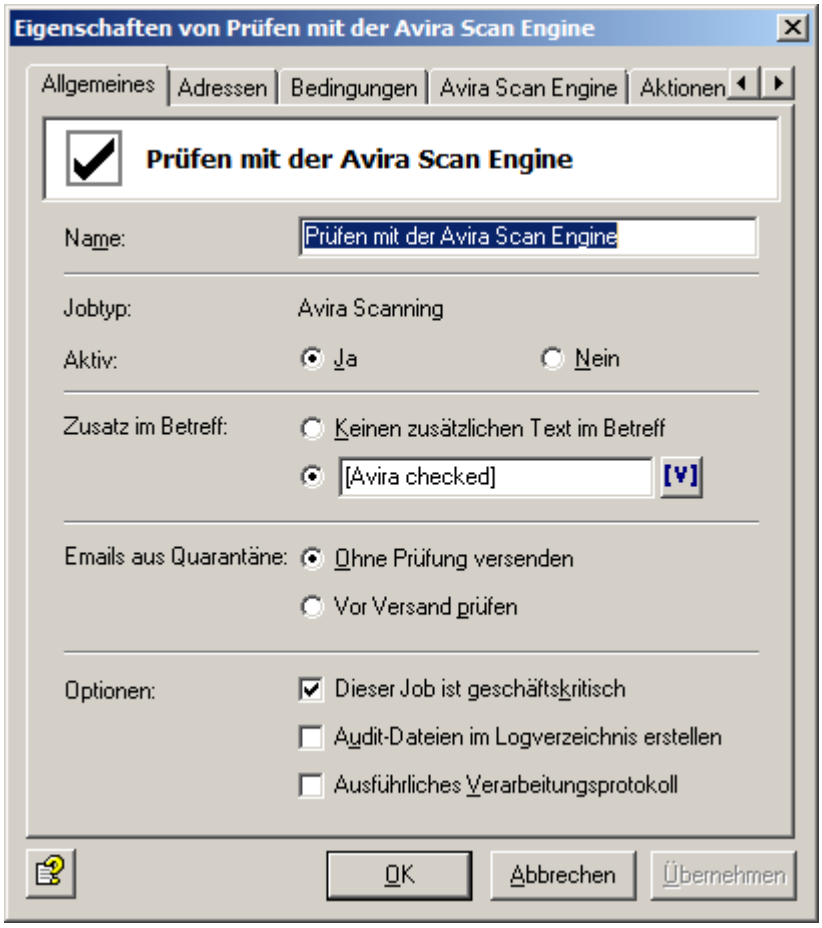
Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen in der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

6. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Email gefunden hat.
7. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.
   Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
8. Auf der Registerkarte **Details** können Sie den Job näher beschreiben.
9. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Adresslisten - Seite 124
Job-Bedingungen - Seite 151
Einstellungen für einen individuellen Avira Server - Seite 111

Allgemeine Einstellungen für die Virenprüfung



- Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.
- Dieser Job kann auch solche Emails erneut kontrollieren, die aus der Quarantäne versendet werden: **Vor Versand prüfen**.

Hinweis

Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

- **Dieser Job ist geschäftskritisch**: Aktivieren Sie diese Option für unternehmenskritische Jobs wie Virenprüfung.
- **Audit-Dateien im Logverzeichnis erstellen**: Aktivieren Sie diese Funktion wenn eine Nachweispflicht besteht oder Sie einen Job testen möchten.

Verwandte Themen:

Emails aus der Quarantäne senden - Seite 24

Geschäftskritische Jobs

Ein Job ist **geschäftskritisch**, wenn die Email bei einem Verarbeitungsfehler - wie beispielsweise bei fehlendem Virenscanner - in den BADMAIL-Bereich abgelegt werden soll.

Warnung
Solange der Verarbeitungsfehler nicht behoben ist, wird bei dieser Option **jede** Email (eingehend oder ausgehend) in den BADMAIL-Bereich überführt.

Ein Job ist **nicht geschäftskritisch**, wenn das Ergebnis des Jobs im Falle eines Verarbeitungsfehlers bei der betreffenden Email ignoriert werden soll. Die Email wird in diesem Fall dem nächsten Job zur Bearbeitung übergeben.

Jeder Verarbeitungsfehler wird im Windows Event Log eingetragen.

Tritt der Verarbeitungsfehler fünf Mal hintereinander auf, wird der Job deaktiviert. Der deaktivierte Job wird nach 15 Minuten automatisch wieder gestartet.

Die Standardeinstellung für fast alle Jobs ist **nicht** geschäftskritisch. Welche Jobs als unternehmenskritisch gelten, sollte in den Firmenrichtlinien festgelegt werden.

Jobverarbeitungsprotokoll

Mit dem Verarbeitungsprotokoll beobachten Sie die Verarbeitung der Emails durch den Job. Schalten Sie diese Funktion ein, wenn evtl. eine Nachweispflicht besteht, oder wenn Sie einen Job testen wollen.

Wenn Sie diese Option aktivieren, wird für jede bearbeitete Email in eine Textdatei geschrieben, ob und wie der Job die jeweilige Email bearbeitet hat. Diese Protokoll-Textdatei wird im Installationsverzeichnis von Avira Exchange Security im Ordner *Log* abgelegt. Die Protokollierung wird pro Job definiert, die Textdatei enthält aber die Informationen aller Jobs, für die **Verarbeitung protokollieren** eingeschaltet ist. Für jeden Tag wird eine separate Textdatei angelegt.

Name der Textdatei: *Audit_all_<Datum der letzten Änderung>.log*, z. B. *Audit_all_20050909.log*

Die einzelnen Informationen über die bearbeitete Email sind mit Semikolons getrennt und können daher manuell oder automatisch ausgewertet werden:

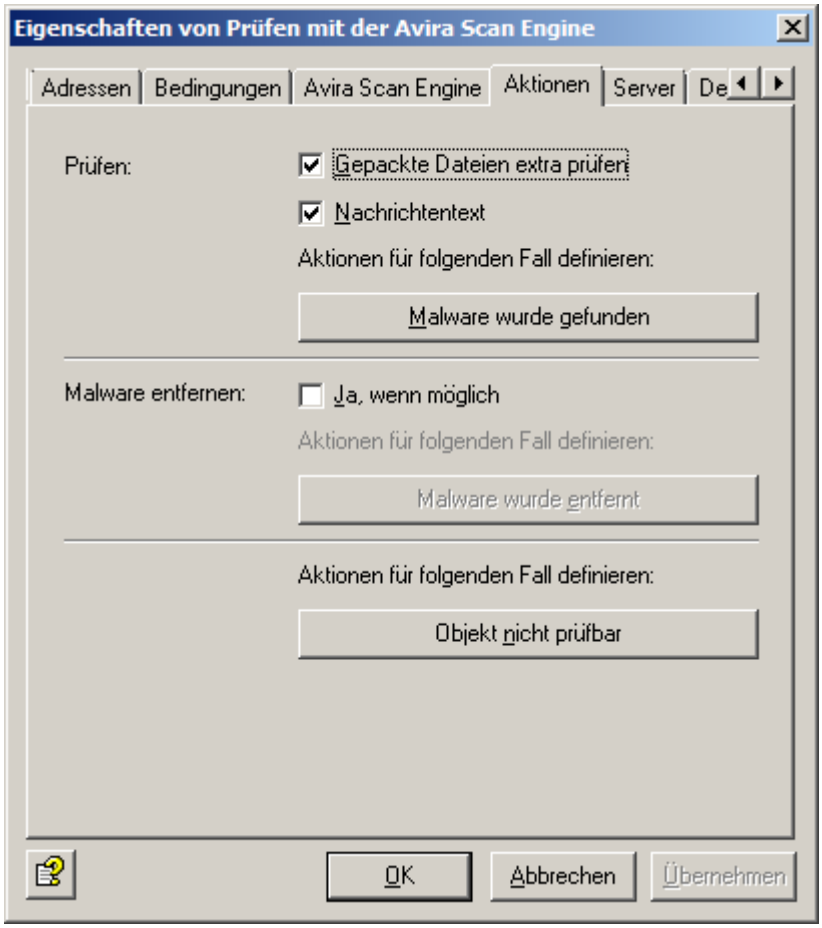
1. Datum und Uhrzeit der Bearbeitung der Email
2. Job-ID
3. Jobname
4. Message-ID
5. SMTP-Absender
6. SMTP-Empfänger
7. Ergebnis der Prüfung durch Avira Exchange Security
    - Restricted - Email entspricht den definierten Restriktionen
    - Unrestricted - Email entspricht nicht den definierten Restriktionen

Empfängergruppen werden aufgelöst. Für jeden Empfänger wird eine eigene Zeile in die Datei geschrieben.

Aktionen für die Virenprüfung

Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen ausgeführt werden, wenn der Job eine virenverseuchte Email gefunden hat.

Beispiel:



Dieser Job soll die Email auf Viren prüfen, aber nicht versuchen, die Email bzw. den Anhang von diesen Viren zu reinigen. In der Regel sind alle Virenscanner zu einer Reinigung in der Lage. Da es in der Praxis aber kaum noch vorkommt, dass Viren versehentlich von bekannten Kommunikationspartnern versendet werden, sondern es meist unerwünschte Emails sind, die gleichzeitig Viren enthalten, ist es effektiver, virenverseuchte Anhänge sofort unter Quarantäne zu stellen.

Hinweis

Da der Job lediglich eine Virenprüfung durchführen soll, müssen Sie die Avira Scan Engine entsprechend konfigurieren. Wählen Sie unter **Basiskonfiguration** › **Utility-Einstellungen** › **Avira Scan Engine** die gewünschte Engine aus und deaktivieren Sie das Feld **Alternativer Reinigungsparameter**. Aktivieren Sie dieses Feld dann, wenn der Job die Email bzw. den Anhang bei einem gefundenen Virus bereinigen soll.

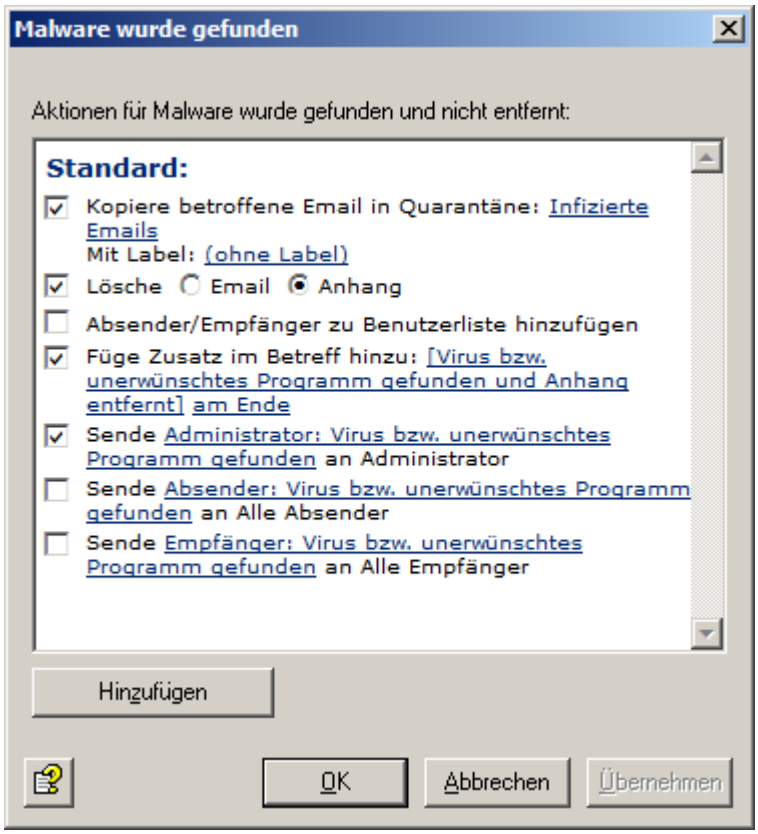
Definieren Sie, wie mit nicht scanbaren Objekten verfahren werden soll.

Nachdem Sie festgelegt haben, was genau geprüft werden soll, definieren Sie zwei unterschiedliche Aktionen:

1. **Malware wurde gefunden**: Für den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte.
2. **Malware wurde entfernt**: Für den Fall, dass die Reinigung der Datei erfolgreich verlaufen ist und der Virus entfernt wurde (sofern Sie diese Option ausgewählt haben).

Die Konfiguration der Aktionen ist in beiden Fällen identisch. Das folgende Beispiel bezieht sich auf den ersten Fall.

Aktionen bei Malware-Fund


Malware wurde gefunden
Aktionen für Malware wurde gefunden und nicht entfernt:
Standard:
Kopiere betroffene Email in Quarantäne: Infizierte Emails
Mit Label: (ohne Label)
Lösche Email Anhang
Absender/Empfänger zu Benutzerliste hinzufügen
Füge Zusatz im Betreff hinzu: [Virus bzw. unerwünschtes Programm gefunden und Anhang entfernt] am Ende
Sende Administrator: Virus bzw. unerwünschtes Programm gefunden an Administrator
Sende Absender: Virus bzw. unerwünschtes Programm gefunden an Alle Absender
Sende Empfänger: Virus bzw. unerwünschtes Programm gefunden an Alle Empfänger
Hinzufügen
OK
Abbrechen
Übernehmen

Eine Kopie der Email wird in die Quarantäne verschoben, und die betroffenen Anhänge werden gelöscht. Die Email wird nur dann dem Empfänger zugestellt, wenn der Nachrichtentext virenfrei war und der Anhang gelöscht werden konnte. Eine Benachrichtigung über den Virus wird an den Administrator gesendet. Diese Benachrichtigung wird aus der Auswahlliste der möglichen Benachrichtigungen ausgewählt; die Liste kann individuell über die HTML-Toolbar oder direkt mit HTML-Formatierungsbefehlen gestaltet werden.

Hinweis

Prüfen Sie, ob an Ihr Unternehmen gesendete Viren-Emails häufig auch Emails mit unerwünschtem Inhalt sind. Wenn dies der Fall ist, sollte idealerweise unverzüglich die gesamte

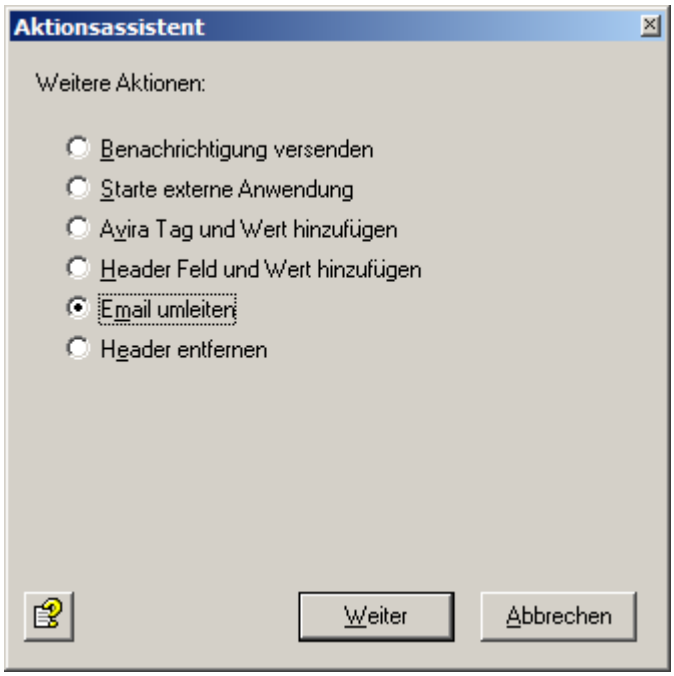
Email und nicht nur der Anhang gelöscht werden. So muss nicht auch noch der verbleibende Nachrichtentext auf unerwünschten Inhalt überprüft werden.

Hinweis

Wenn Sie die Option **Auf Viren prüfen: Nachrichtentext** aktiviert haben und tatsächlich ein Virus im Text gefunden wird, so wird die gesamte Email inklusive der Anhänge gelöscht, wenn Sie **Lösche Anhang** gesetzt haben (es wird kein Anhang ohne Nachrichtentext zugestellt). Der betroffene Email-Abschnitt wird generell einzeln gelöscht. Wenn nur der Anhang einen Virus enthält, wird nur der Anhang gelöscht.

Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.

Weitere Aktionen bei Malware-Fund



- **Benachrichtigung versenden**: Wählen Sie den Empfänger der Benachrichtigung aus dem Adressbuch aus.
- **Starte externe Anwendung**: Eine neue Anwendung/Applikation kann angegeben werden, damit Aktionen dieser Anwendung ausgeführt werden können. Für den Start einer externen Anwendung geben Sie den Pfad und ggf. die notwendigen Parameter an.
- **Avira Tag und Wert hinzufügen**: Während des Verarbeitungsprozesses können Mail-Header-Tags eingesetzt werden, um spezielle Avira Exchange Security-Aktionen ausführen zu lassen. Beispielsweise können einer Email zusätzliche Angaben hinzugefügt werden, die ein nachfolgender Job auswertet. Beim Versenden der Email an den ursprünglichen Empfänger werden die Angaben des Mail-Header-Tags entfernt.
- **Header Feld und Wert hinzufügen**: Definieren Sie ein neues X-Header-Feld und wählen Sie die Variable aus, die eingefügt werden soll, z. B. um das Ergebnis einer Email-Filter-Analyse als

Wert auszugeben. Im Gegensatz zum Mail-Header-Tag bleiben diese Informationen auch beim Versand der Email an den ursprünglichen Empfänger erhalten.

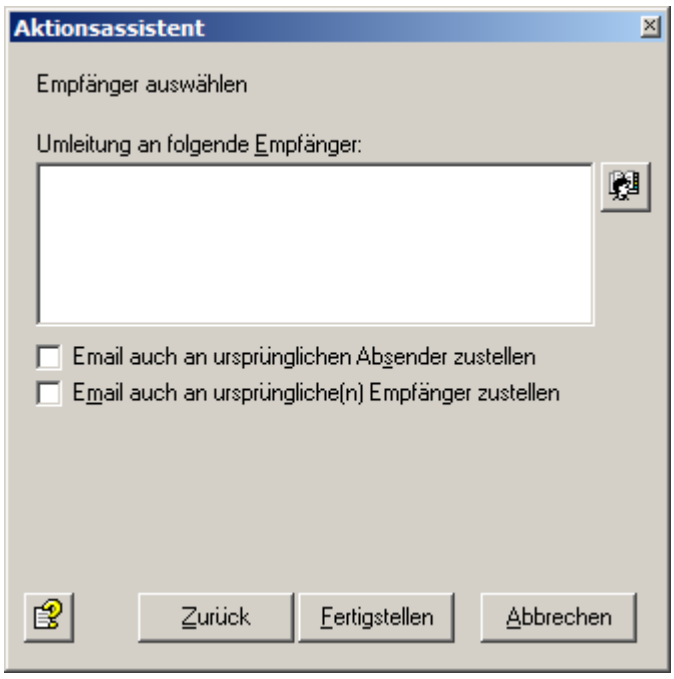
- **Email umleiten**: Wählen Sie den Empfänger der umgeleiteten Email aus dem Adressbuch aus. **Email umleiten** ist nicht voreingestellt, die Option wird Ihnen lediglich als weitere Aktion vorgeschlagen.

Hinweis

Anmerkung zu **Email umleiten**: Wenn Sie eine TNEF-Mail an eine externe Adresse umleiten, erhalten Sie dort eine leere Email, evtl. mit einem *winmail.dat*-Anhang. Das TNEF-Format wird von Exchange verwendet, wenn ein Outlook-Benutzer (nicht Outlook Express!) innerhalb einer Exchange-Organisation eine Email sendet. Bei der Kommunikation über das Internet bzw. bei Verwendung anderer Email-Programme wird dieses Format nicht verwendet.

- **Header entfernen**: Die X-Header-Felder der Email werden entfernt. Sie können diese Aktion verwenden, wenn Sie die X-Header-Felder entfernen möchten, die zuvor auf anderen Server festgelegt wurden.

Klicken Sie **Weiter** und nehmen Sie je nach ausgewählter Option weitere Konfigurationen vor. Bei **Email umleiten** haben Sie folgende Möglichkeiten:



Klicken Sie auf das Symbol für das Adressbuch , um weitere Empfänger auszuwählen oder eigene Adressen zu definieren. Wenn Sie die Email zusätzlich auch dem ursprünglichen Empfänger oder dem ursprünglichen Absender zustellen möchten, aktivieren Sie jeweils das zugehörige Kontrollkästchen.

Klicken Sie **Fertigstellen**, um die Aktionseinstellungen zu speichern.

5.2 Suche im Informationsspeicher-Jobs

Für Microsoft Exchange Server muss ab 2013 ein separater EWS-Benutzer mit bestimmten Zugriffsrechten angelegt werden.

Legen Sie einen EWS-Benutzer mit bestimmten Zugriffsrechten an:

1. Öffnen Sie die Exchange Management Console, beispielsweise über `https:\\localhost\ecp`.
2. Legen Sie einen neuen Benutzer (samt Mailbox) an. In diesem Beispiel hat der Benutzer den Namen `ews_user`.
3. Öffnen Sie die Exchange Management Shell und weisen Sie dem Benutzer die erforderlichen Rechte zu, indem Sie das Skript*SetEWSPermissions.ps1* im Verzeichnis *Avira Exchange Security/Bin* aufrufen. Um die Zugriffsrechte auf dem Exchange-Server festzulegen, geben Sie Folgendes ein: `SetEWSPermissions.ps1 -User "user name"` (ohne Domain). Beispiel: `SetEWSPermissions.ps1 -User ews_user`

Hinweis

Zugriffsrechte können nur für öffentliche Ordner eingerichtet werden, die gegenwärtig im Informationsspeicher verfügbar sind. Wenn die datenbankrelevanten Einstellungen für die öffentlichen Ordner (z. B. durch Hinzufügen eines neuen Ordners) geändert werden, muss das Skript erneut ausgeführt werden, um die erforderlichen Rechte für die geänderten Elemente festzulegen.

Geben Sie in den Avira Server Einstellungen den `ews user` einschließlich des Passworts an:

ALLGEMEINE EINSTELLUNGEN -> Avira Server Einstellungen -> Registerkarte OPTIONEN. Geben Sie den Benutzernamen einschließlich der Domain ein, z. B. `ews_user@mydomain.com`.

Neben der Virenprüfung auf Transport-Ebene ist Avira Exchange Security auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen. Diese Prüfung bezieht sich nicht auf den ein- oder ausgehenden Email-Verkehr, sondern auf die auf dem Server vorhandenen Email-Dateien bzw. solche, die nicht mit dem Transport-Agenten in Berührung kommen oder gekommen sind, z. B. Entwürfe.

Beim Informationsspeicher-Scan handelt es sich um serverweite Einstellungen. Daher steht für jeden Server immer nur ein Suche im Informationsspeicher-Job zur Verfügung, und nicht beliebig viele wie bei Avira Prüfung-Jobs.

Die Virenprüfung des MS Exchange Informationsspeichers erfolgt über die Microsoft Virus Scanning API 2.0/2.5. Weitere Informationen hierzu finden Sie unter *http://support.microsoft.com/kb/285667/EN/*.

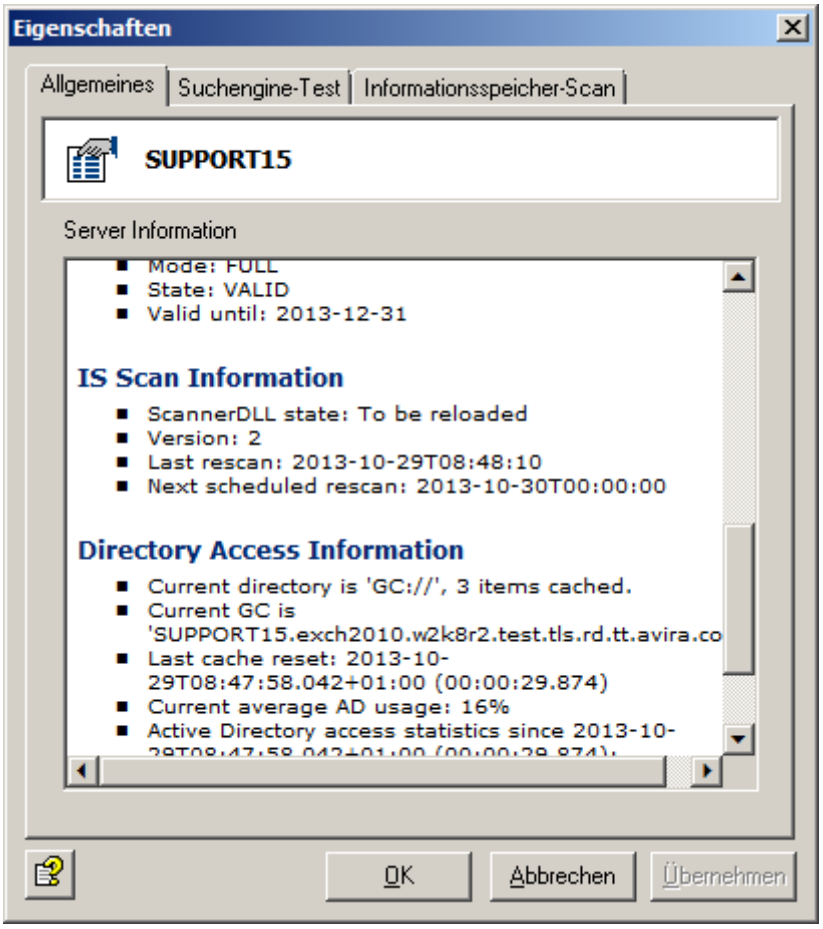
Warnung

Bei Nachrichten, die durch den Informationsspeicher-Scan blockiert werden, kann es bei Datensicherungen des Informationsspeichers zu Fehlermeldungen kommen.

Warnung
Das Beenden oder Deinstallieren von Avira Exchange Security sowie das Anhalten der Suche im Informationsspeicher-Jobs deaktiviert nicht nur den aktiven Virenschutz des Informationsspeichers, sondern hebt auch die Sperrung virulenter Inhalte auf.

5.2.1 Informationsspeicher-Status

1. Klicken Sie auf **Avira Monitor** > **Server** > **Server Status**.
2. Wechseln Sie zur Registerkarte **Allgemein**.



ScannerDLL state zeigt *Loaded* an, sobald der Informationsspeicher-Scan aktiv ist.

Version zeigt die Version des Informationsspeicher-Scans an. Jeder Neustart erhöht diesen Wert.

Last rescan zeigt, wann die letzte Versionsaktualisierung erfolgte sowie Zeit und Datum des letzten Neustarts.

Next scheduled rescan zeigt Zeit und Datum der nächsten erneuten Überprüfung, falls eine geplant ist.

5.2.2 Informationsspeicherscan neu starten

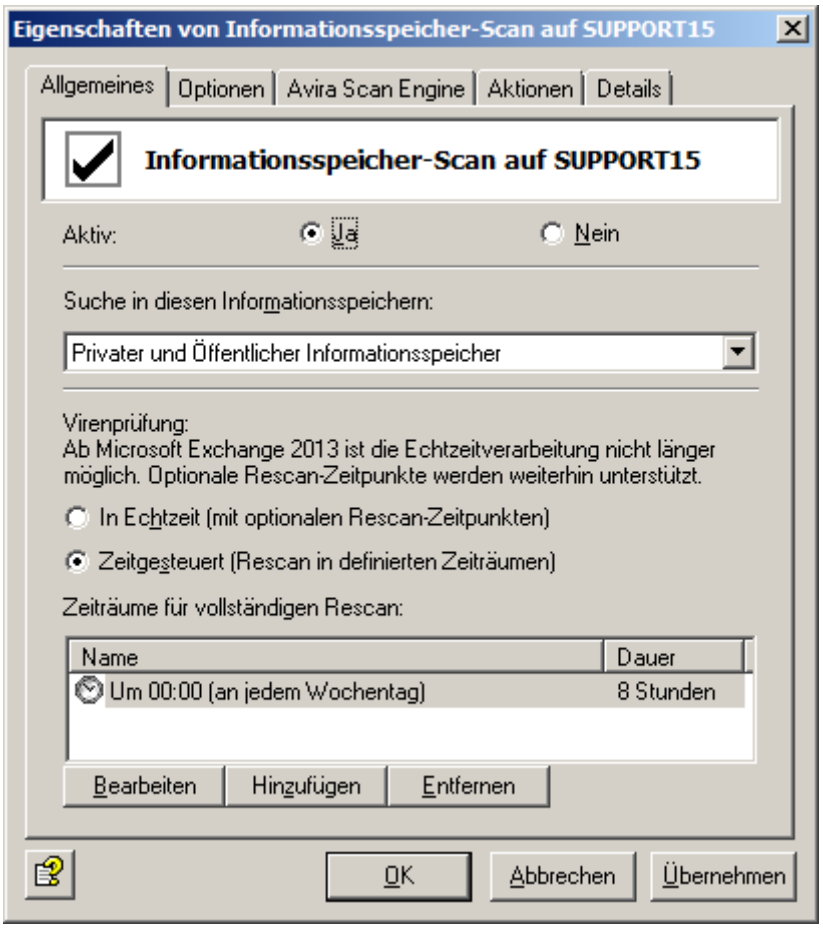
Warnung
Durch einen Neustart des Scans werden sämtliche Elemente im Informationsspeicher neu überprüft. Diese Prüfung kann sehr zeit- und ressourcenintensiv sein. Es ist daher empfehlenswert, den Neustart zu Tagesrandzeiten und in Abhängigkeit der Virenscanneraktualisierung zu starten.

1. Klicken Sie auf **Avira Monitor** > **Server** > **Server Status**.
2. Klicken Sie auf die Registerkarte **Suche im Informationsspeicher-Scan**.
3. Klicken Sie **Jetzt scannen**.

5.2.3 Einen Suche im Informationsspeicher-Job aktivieren

Warnung
Nach dem Aktivieren/Deaktivieren des Suche im Informationsspeicher-Jobs kann es bis zu zwei Minuten dauern, bis der Exchange Store die Änderung registriert.

1. Doppelklicken Sie den Job Suche im Informationsspeicher unter **Richtlinien-Konfiguration**.



2. Klicken Sie **Ja** auf der Registerkarte **Allgemein**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.

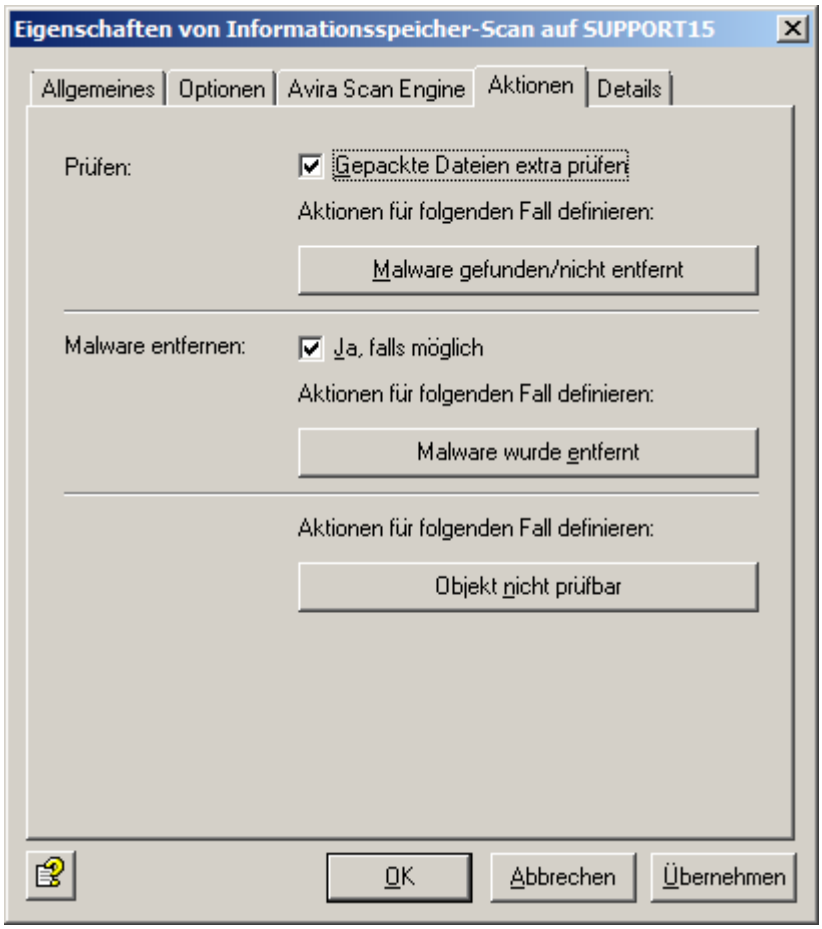
- **Suche in diesen Informationsspeichern**: Wählen Sie aus der Dropdown-Liste die Speicher aus, die geprüft werden.
- **Virenprüfung**: Aktivieren Sie die Virenprüfung **In Echtzeit** oder **Zeitgesteuert**.
- **Zeiträume für vollständigen Rescan**: Wenn Sie die zeitgesteuerte Virenprüfung verwenden, können Sie Zeiträume für die Virenprüfung festlegen.

3. Auf der Registerkarte **Optionen** können Sie die Optionen **Job ist geschäftskritisch** und **SMTP-Server für Benachrichtigungen verwenden** aktivieren.
4. Auf der Registerkarte **Avira Scan Engine** können Sie die Liste der Suchengines anpassen und das Verhalten im Fehlerfall festlegen.
   - Mindestens eine Suchengine muss fehlerfrei laufen
   - Alle Suchengines müssen fehlerfrei laufen
5. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Email gefunden hat.
6. Auf der Registerkarte **Details** können Sie den Job näher beschreiben.
7. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Geschäftskritische Jobs - Seite 40

Aktionen für IS-Jobs festlegen

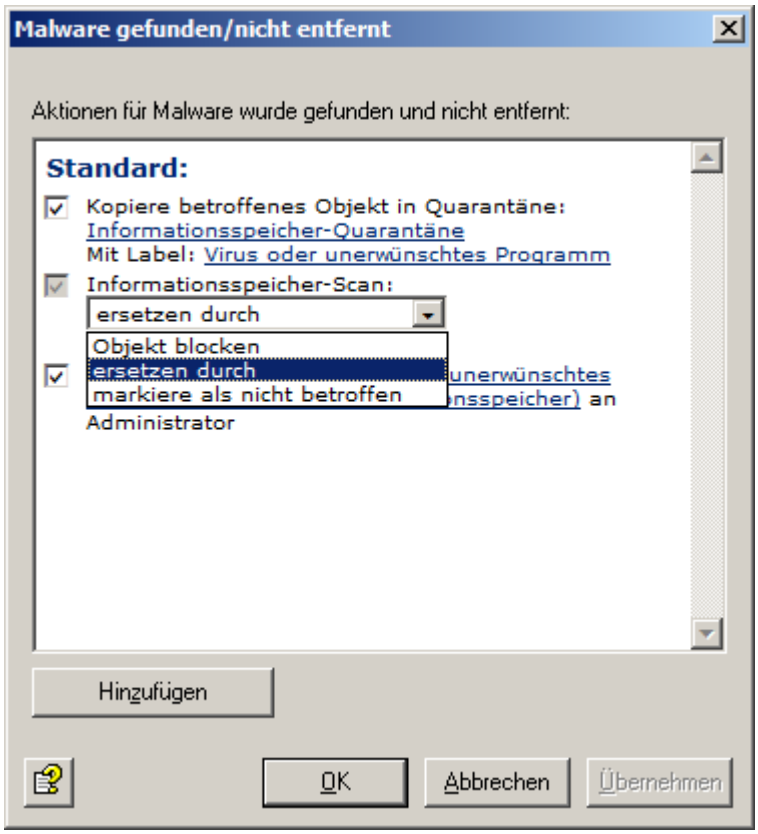


Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine virenverseuchte Email gefunden hat.

- **Gepackte Dateien extra prüfen**: Damit wird ein interner Entpacker die gepackten Dateien zunächst extrahieren und danach einzeln dem Virenscanner zuführen.
- **Malware entfernen**: Wenn Sie möchten, dass der IS-Job versucht, die Malware zu entfernen, aktivieren Sie die Option **Ja, falls möglich**.
- Sie haben folgende Möglichkeiten:
  - **Malware gefunden/ nicht entfernt**
  - **Malware wurde entfernt**
  - **Objekt nicht prüfbar**

Aktionen bei Malware-Fund

Malware gefunden/nicht entfernt: Für den Fall, dass ein Virus gefunden wurde und die Datei nicht erfolgreich gereinigt werden konnte.

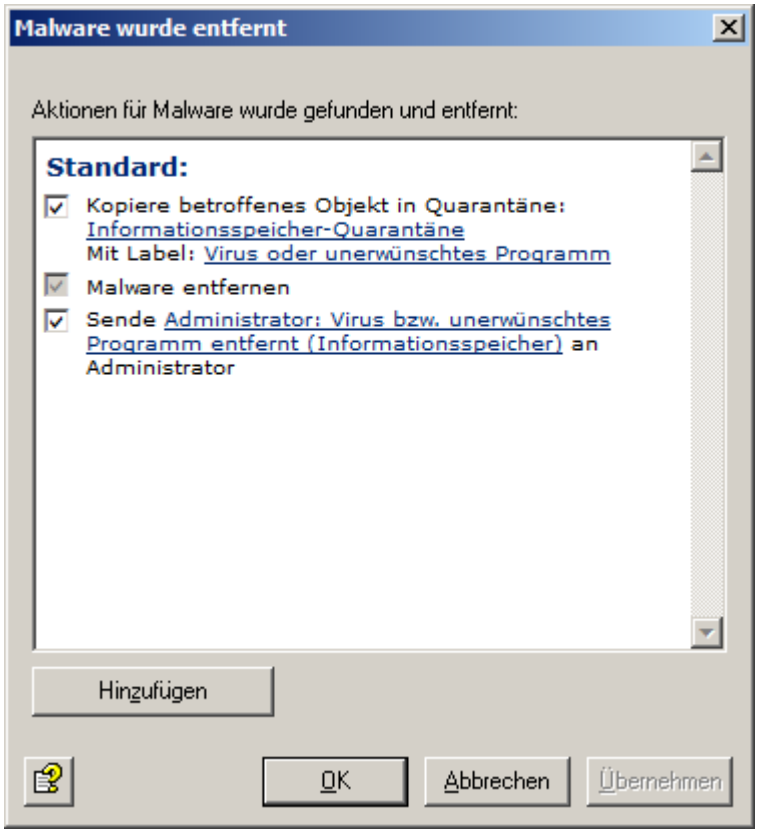


1. Zunächst wählen Sie, ob eine Kopie des Objektes unter Quarantäne gestellt und mit einem Label versehen werden soll.

   Für den Informationsspeicher-Scan steht eine spezielle Standard-Quarantäne zur Verfügung.
2. Legen Sie fest, wie der IS mit dem Objekt verfahren soll.
   - **Objekt blocken**: Das Blockieren verbietet den Zugriff auf das gesamte Nachrichtenobjekt. Bei aktuellen Microsoft Email Clients wird beim Versuch, eine solche Nachricht zu öffnen, eine entsprechende Meldung generiert. Bei anderen/älteren Email-Clients kann es zu unterschiedlichen Rückmeldungen kommen. Die blockierten Nachrichten können allerdings jederzeit über den Client gelöscht werden.
   - **Ersetzen durch**: Beim Ersetzen wird das virulente Element der Nachricht (z. B. Dateianhang) gegen einen Textvermerk ausgetauscht. Das virulente Element wird gelöscht.
   - **Markiere als nicht betroffen**: In Ausnahmefällen kann entschieden werden, dass bei einem gefundenen Virus das entsprechende Element nicht als virulent markiert wird. Nachfolgende Virenprüfungen werden das Element dann wiederum als virulent erkennen. Diese Aktion ist nur in Testumgebungen sinnvoll, da hier kein Schutz des Anwenders gewährleistet ist.
3. Geben Sie an, ob eine Benachrichtigung über den Virus an den/die Administrator/en versendet wird.
4. Klicken Sie **Hinzufügen**, um zusätzliche Aktionen auszuführen, z. B. um dem Empfänger eine Benachrichtigung zu senden oder um eine externe Anwendung zu starten.

Aktionen bei entfernter Malware

Malware wurde entfernt: Im Fall, dass ein Virus gefunden wurde und die Datei erfolgreich gereinigt werden konnte.

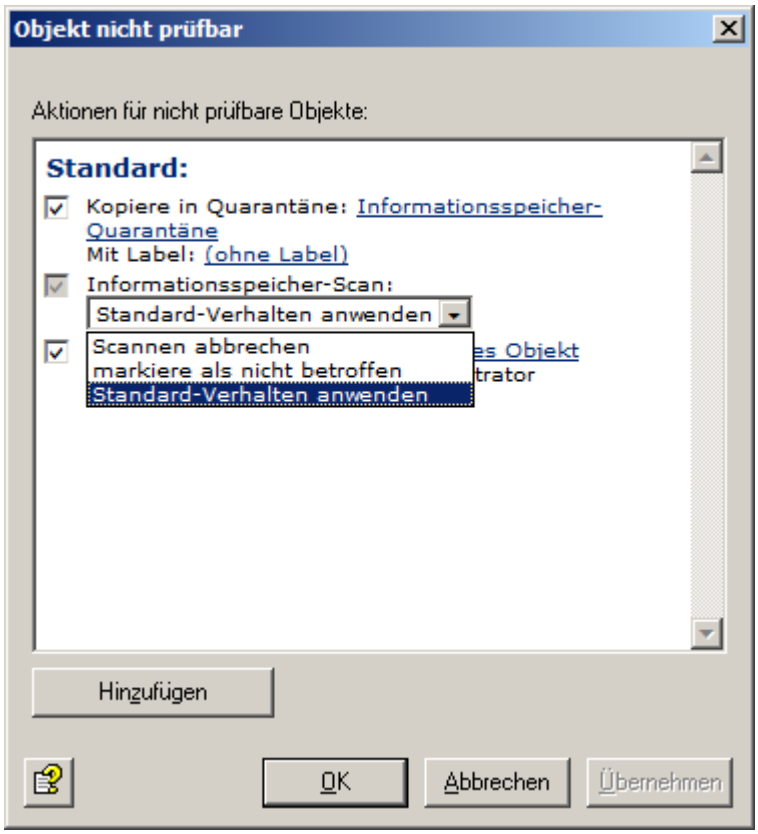


1. Zunächst wählen Sie, ob eine Kopie des Objektes unter Quarantäne gestellt und mit einem Label versehen werden soll.

   Das Objekt wird vor der Reinigung kopiert, d .h. es befindet sich in seinem ursprünglichen Zustand in der Quarantäne.
2. Geben Sie an, ob Benachrichtigung über den Virus an den/die Administrator/en versendet wird.
3. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen auswählen.

Aktionen bei nicht prüfbaren Objekten

Objekt nicht prüfbar: Behandelt den Fall, dass die Dateien nicht geprüft werden konnten. So lässt sich beispielsweise das Verhalten von Avira Exchange Security beim Auffinden verschlüsselter Objekte beeinflussen, welche naturgemäß nicht einsehbar und damit nicht auf Viren prüfbar sind.

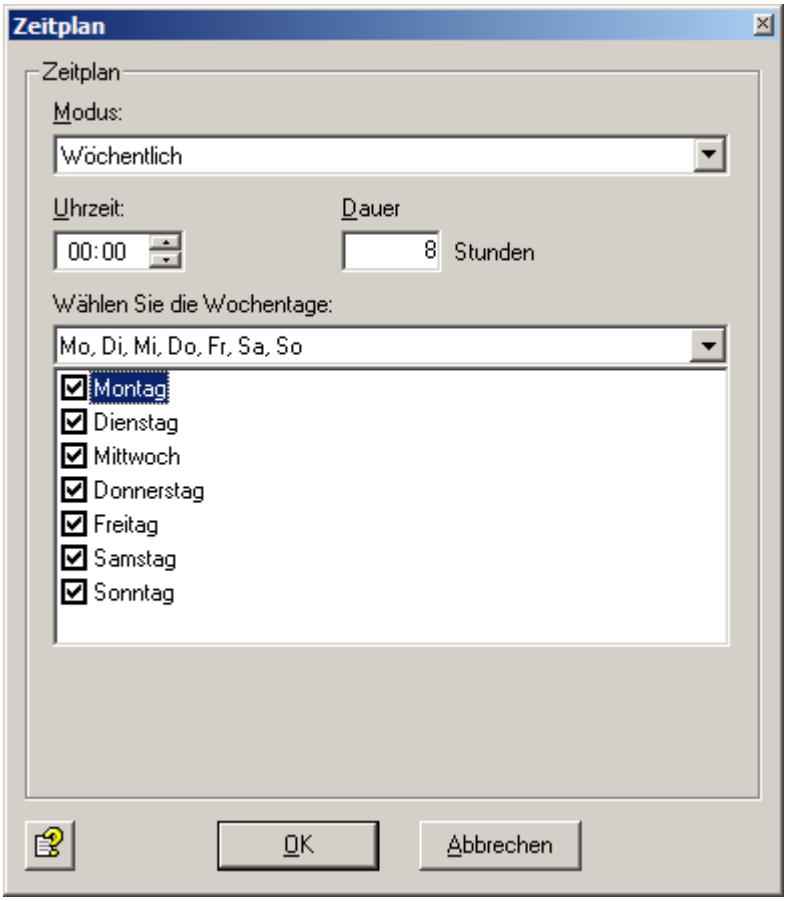


1. Zunächst wählen Sie, ob eine Kopie des Objektes unter Quarantäne gestellt und mit einem Label versehen werden soll.
2. Legen Sie fest, wie der IS mit dem Objekt verfahren soll.
   - **Scannen abbrechen**: Das Objekt wird beim nächsten Scanvorgang erneut überprüft. Der Zugriff ist dabei blockiert, falls vorhergehende Scanvorgänge das Objekt als virenfrei behandelt haben.
   - **markiere als nicht betroffen**: Das Objekt wird behandelt, als sei es virenfrei. Es wird erst beim nächsten Neustart der Virenprüfung erneut geprüft.
   - **Standard-Verhalten anwenden**: Das Objekt wird behandelt., wie unter **Basiskonfiguration** › **Avira Server** › **Allgemein** für die Option **Bei nicht scanbaren Elementen folgende Aktion ausführen** eingestellt wurde.
3. Geben Sie an, ob eine Benachrichtigung über den Virus an den/die Administrator/en versendet wird.
4. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen auswählen.

Zeitplan für Suche im Informationsspeicher erstellen

Sie können für den Neustart des Suche im Informationsspeicher einen Zeitplan erstellen.

1. Doppelklicken Sie den Job Suche im Informationsspeicher unter **Richtlinien-Konfiguration**.
2. Aktivieren Sie den Prüfungsmodus **Zeitgesteuert**.



3. Legen Sie den Zeitplan fest.
   - Modus
   - Uhrzeit
   - Wochentage
4. Klicken Sie **OK**.

5.3 Avira geschützte Anhangserkennung

Damit Avira-Jobs Emails verarbeiten können, müssen die Emails vollständig entpackt sein. Bei passwortgeschützten Archiven ist kein Entpacken möglich. Daher werden Emails mit solchen Dateianhängen standardmäßig von einem Virenscan-Job als "nicht prüfbar" geblockt und in der BADMAIL-Quarantäne abgelegt.

Um diese Aktion zu verhindern, verwenden Sie den Job Avira geschützte Anhangserkennung. Der Job reagiert auf Emails mit passwortgeschützten Archiven und führt die in der Registerkarte **Aktionen** konfigurierten Jobaktionen aus. Dadurch können passwortgeschützte Archive regelbasiert behandelt werden. Beispielsweise werden solche Emails für bestimmte Personen/ Personengruppen geblockt während sie für andere zugestellt werden.

Da die Emails im letzteren Fall ungeprüft zugestellt würden, sollten die Emails vor der Zustellung von einem Virenscan-Job geprüft werden. Dazu markiert der Avira Prüfung-Job die Emails, in denen passwortgeschützte Archive enthalten sind. Ein nachfolgender Virenscan-Job behandelt

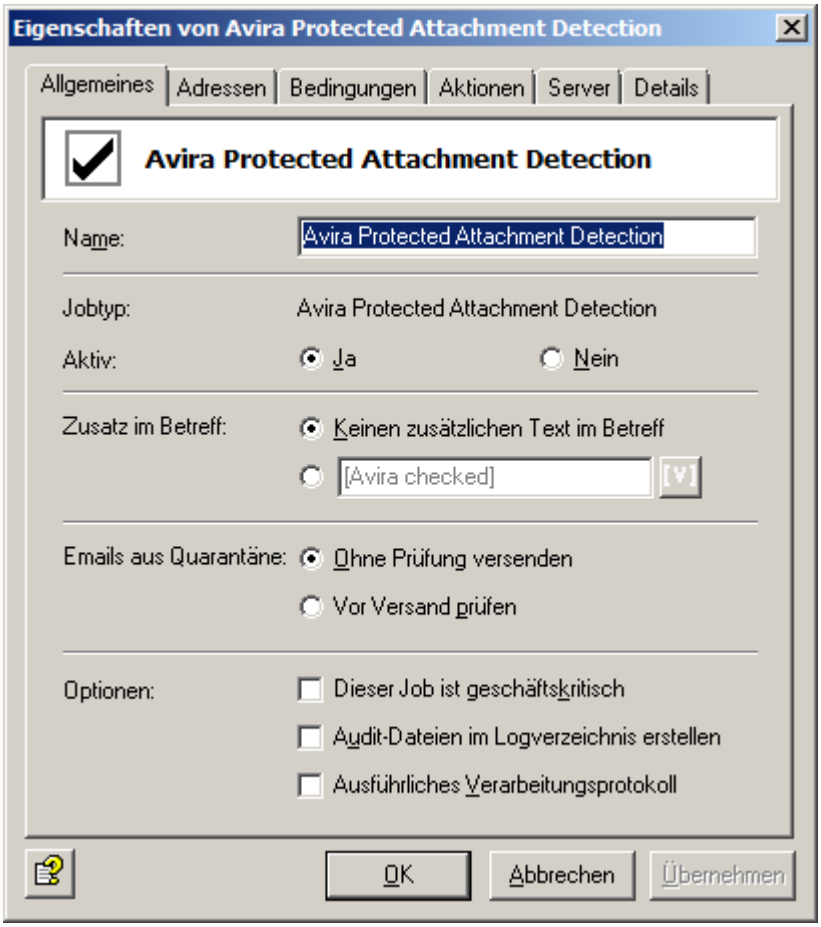
die Emails aufgrund dieser Markierung wie eine "normale" Email und kann ohne diesen Job auftretende Verarbeitungsfehler (*DENIED*) ignorieren.

Alternativ definieren Sie eine Aktion für nicht scanbare Objekte unter **Mail-Transport-Jobs › Prüfen mit der Avira Scan Engine › Aktionen › Aktionen für folgenden Fall definieren: Objekt nicht prüfbar**

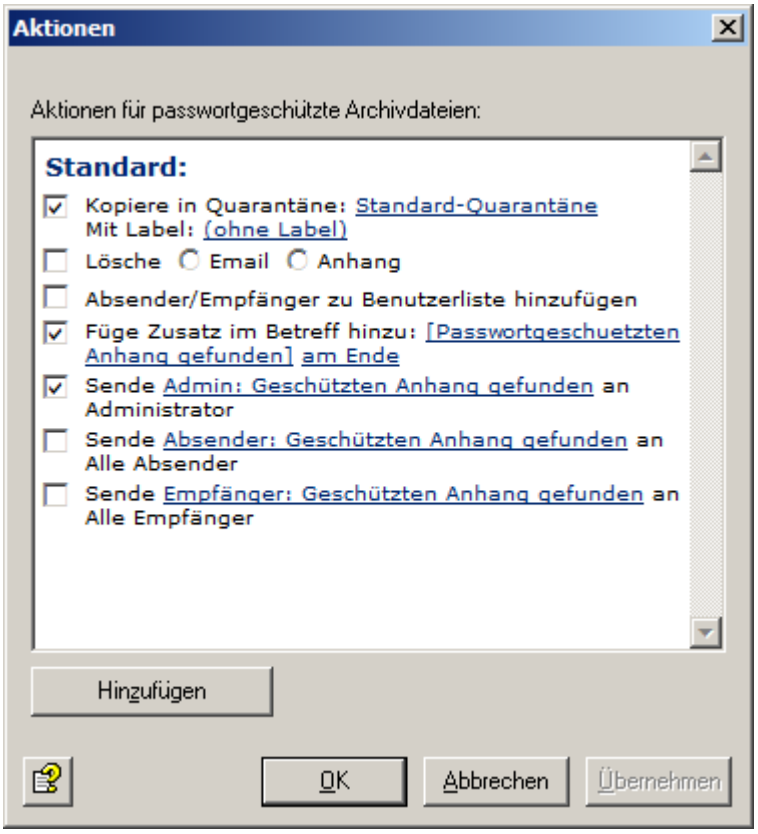
Warnung
Der Virenscanner prüft nicht die in Archiven enthaltenen Dateien auf Virenbefall.

5.3.1 Einstellungen für einen Avira geschützte Anhangserkennung-Job

1. Klicken Sie mit der rechten Maustaste **Mail-Transport-Jobs** und wählen Sie **Neu** › **Avira geschützte Anhangserkennung**.



2. Aktivieren Sie den Job.
   In diesem Beispiel werden nur die jobspezifischen Details erläutert.
3. Wählen Sie die Aktionen aus.



Mit der Voreinstellung des Jobs wird ein Zusatz in den Betreff der Email eingefügt und dem Administrator eine Benachrichtigung zugestellt. Eine Email-Kopie wird in der Standard-Quarantäne abgelegt, die Email jedoch nicht blockiertt (Option **Lösche Email** ist deaktiviert). Je nach Konfiguration wird sie an einen nachfolgenden Virenscan-Job übergeben und anschließend dem Empfänger zugestellt.

Wenn Emails blockiert und den Empfängern nicht zugestellt werden sollen, aktivieren Sie die Option **Lösche Email**. Die Email verbleibt dann bis zur Prüfung und Freigabe durch den Administrator in der Standard-Quarantäne.

5.4 Avira Anhangsfilterung-Jobs

Unter **Richtlinien-Konfiguration** > **Jobvorlagen** finden Sie verschiedene Jobs für das Blockieren diverser Dateiformate.

- **Blocke Archive, außer ZIP-Dateien**: Alle komprimierten Formate, außer ZIP-Dateien
- **Blocke verdächtige Anhänge**: Bekannte gefährliche Anhänge wie Nimda etc.
- **Blocke Videodateien**: Videoformate
- **Blocke Sounddateien**: Soundformate
- **Blocke ausführbare Dateien**: Ausführbare Dateien (exe, com, etc.)
- **Blocke Bilddateien**: Grafikformate

Die Datei muss von Avira identifiziert werden. Dafür wird der Fingerabdruck der Datei geprüft, der das binäre Dateimuster, z. B. bei *.exe-Dateien, und/oder die Dateierweiterung (Extension), z. B. bei *.vbs-Dateien, enthält.

Das Ergebnis dieser Prüfung wird mit den verbotenen/erlaubten Fingerabdrücken unter Avira-Einschränkungen verglichen und entsprechend abgewiesen oder zugelassen. Für abgelehnte Dateien werden dann die Aktionen aus dem Job ausgeführt, z. B. bei einer Email mit einem verbotenen Anhang:

- Der verbotene Anhang wird in die Quarantäne kopiert.
- Der Nachrichtentext wird dem Empfänger zugestellt.
- Benachrichtigungen werden an den Administrator und den Absender geschickt.

Folgende Aktionen sind bei einem Avira Anhangsfilterung-Job möglich:

- Gesamte Email in Quarantäne stellen
- Betroffene Anhänge aus Email entfernen
- Betroffene Email löschen und nicht zustellen
- Absender oder Empfänger in Whitelist hinzufügen
- Zusatz im Betreff
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Externe Anwendung ausführen
- Avira Tag und Wert hinzufügen
- Header-Feld und Wert hinzufügen
- Email umleiten
- Header-Feld entfernen

5.4.1 Fingerprints

Ein Fingerprint besteht aus einem Namensmuster und/oder einem Binärmuster.

- **Namensmuster**: Damit können Fingerprints anhand von Dateinamen und -erweiterung (*.exe, ...) konfiguriert werden.
- **Binärmuster**: Damit können Fingerprints anhand von eindeutigen binären Datei-Informationen konfiguriert werden.

Mit dem Namensmuster sind natürlich auch Manipulationen möglich, da (wenn die Anwender davon wissen) einfach die Erweiterung geändert werden kann. Das Binärmuster ist eine eindeutige Zuordnung zu einem Format und lässt sich in der Datei nicht so leicht manipulieren. Somit ist der sichere Weg, ein Dateiformat zu erkennen, die Eingabe eines Binärmusters.

Mit Namensmustern ist es aber möglich, auf neue Virusattacken schnell zu reagieren. Sobald bekannt ist, mit welchen Anhangnamen ein neuer Virus verbreitet wird (Beispiel: *Nimda* Virus = *readme.exe*) kann die Virus-Attacke abgewehrt werden, noch bevor ein Virus Pattern Update des Antivirus Herstellers verfügbar ist. Der Dateiname wird einfach mit dem Namensmuster als neuer Fingerprint angelegt.

Auch das Blockieren individueller Dateien ist möglich. Setzt ein Unternehmen Individualsoftware ein, welche ein eigenes Dateiformat erzeugt, kann dafür ebenfalls ein Fingerprint erstellt und somit beispielsweise verhindert werden, dass solche Dateien das Unternehmen per

Email verlassen. Fingerprints können Sie organisieren und zu einer logischen Kategorie zusammenfassen.

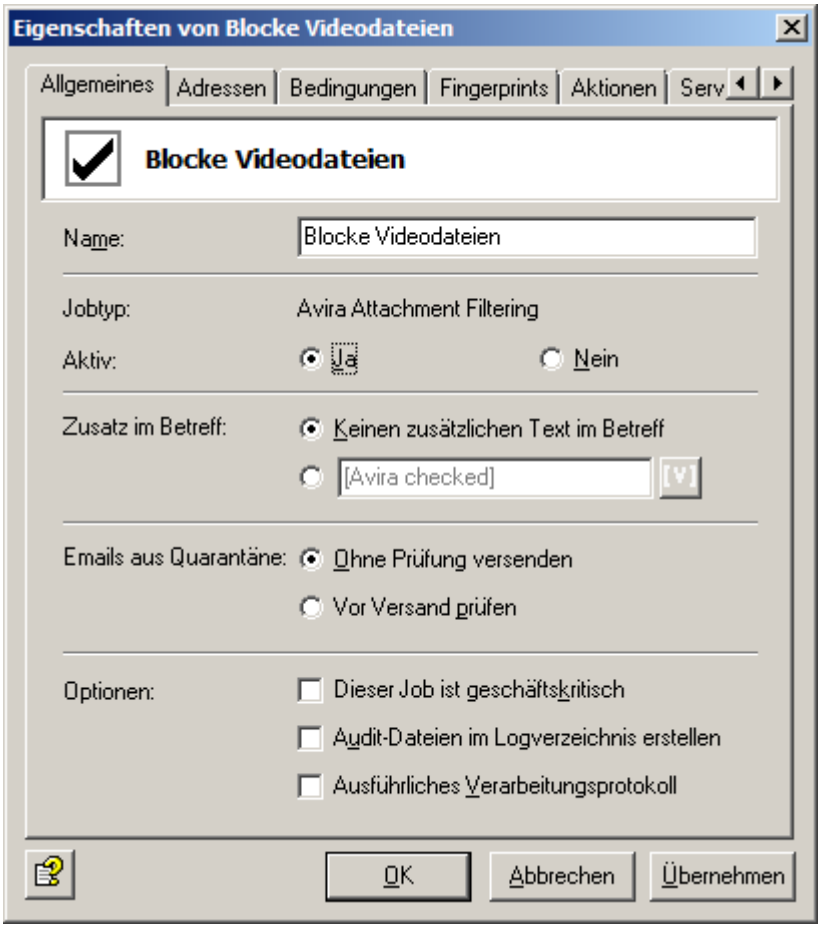
Eine Reihe von vorgefertigten Fingerprints für Standarddateien stehen mit dem Programm automatisch zur Verfügung. Zur Erstellung individueller Fingerprints setzen Sie sich bitte mit dem Support in Verbindung.

5.4.2 Videodateien blockieren

Als Beispiel wird hier der Job **Blocke Videodateien** behandelt.

1. Ziehen Sie den Job **Blocke Videodateien** per Drag-and-Drop in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere allgemeine Einstellungen vorzunehmen.

   Sobald Sie Ihre Einstellungen mit **OK** gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *deaktiviert*.

Dieser Job kann auch solche Emails kontrollieren, die aus der Quarantäne wieder versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

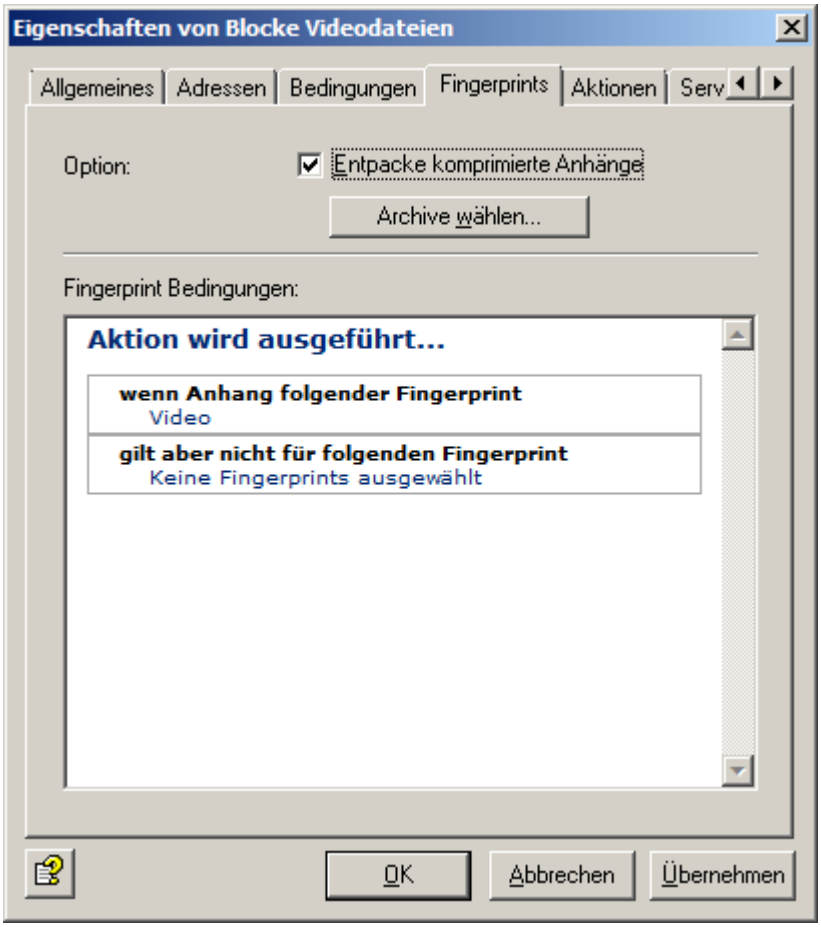
   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

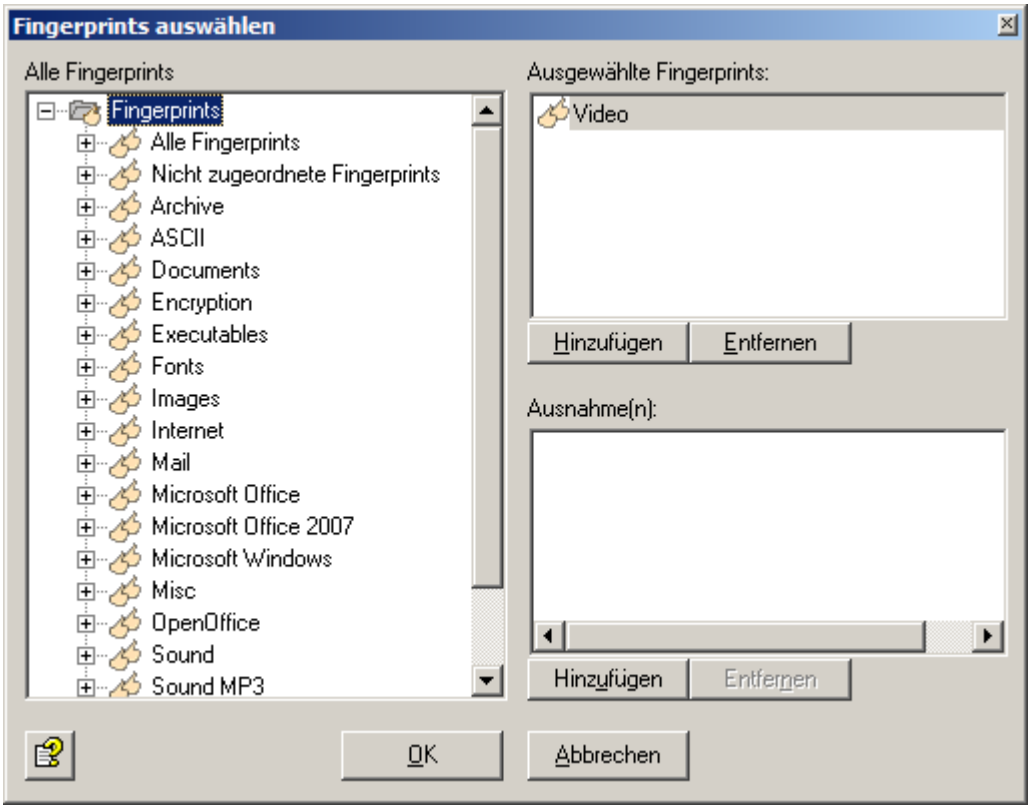
6. Wählen Sie auf der Registerkarte **Fingerprints** die verbotenen Fingerprints aus.



Entpacke komprimierte Anhänge bedeutet, dass der interne Entpacker die Archive öffnet und die darin liegenden Dateien auf die angegebenen Fingerprints untersucht. Ist die

Checkbox nicht aktiviert, wird nur das Archiv als oberste Datei untersucht und als gepacktes Format erkannt.

7. Um die Fingerprint-Bedingungen festzulegen, klicken Sie auf **Video** bzw. **keine Fingerprints ausgewählt**.



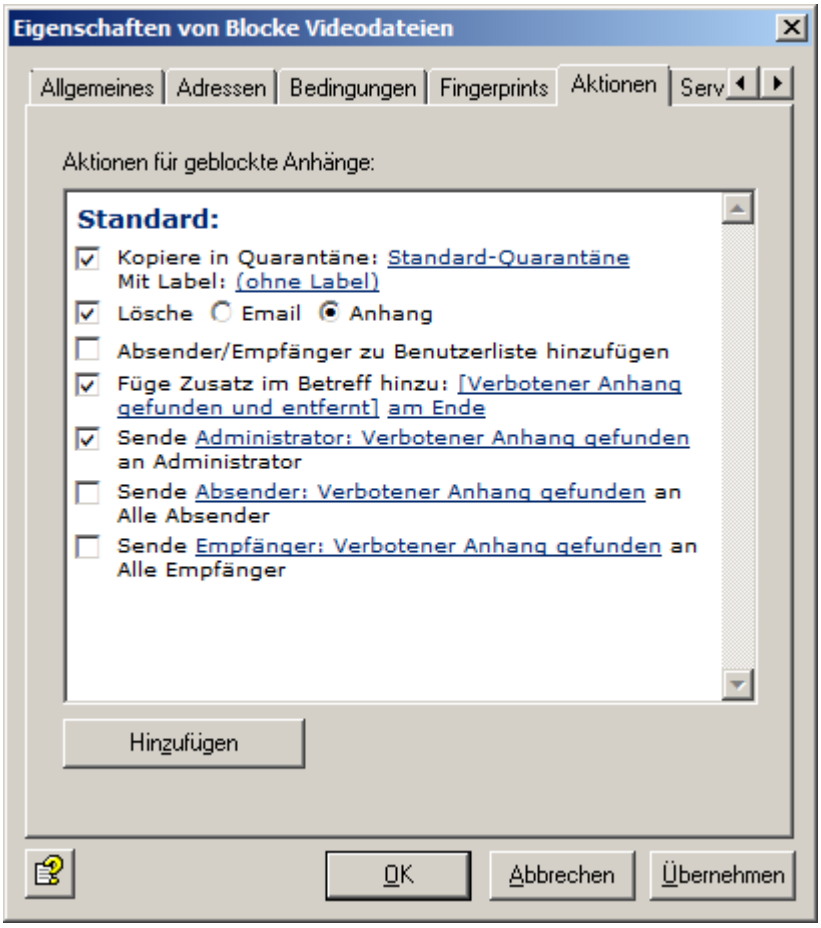
Sie können eine Fingerprint-Kategorie oder einen individuellen Fingerprint aus einer Fingerprint-Liste auswählen.

8. Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das **+** (Plus)-Zeichen.

Hinweis

Sie können eine Kategorie wie z. B. **Video** unter *Ausgewählte Fingerprints* und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter *Ausnahme(n)* eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.

9. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job einen verbotenen Fingerprint als Anhang gefunden hat.



Eine Kopie der Email wird in die Quarantäne verschoben, und die betroffenen Anhänge werden gelöscht. Das bedeutet, dass die Email zwar an den Empfänger zugestellt wird, die verbotenen Anhänge aber entfernt werden. Eine Benachrichtigung über den gefundenen Fingerprint wird an die Administratoren versandt. Diese Benachrichtigung wird aus der Auswahlliste der möglichen Benachrichtigungen ausgewählt; die Liste kann individuell über die HTML-Toolbar oder direkt mit HTML-Formatierungsbefehlen gestaltet werden.

10. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
11. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

    Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
12. Auf der Registerkarte **Details** können Sie den Job näher beschreiben.
13. Klicken Sie die Schaltfläche **Konfiguration speichern** .

5.5 Avira Email-Größenfilterung-Jobs

Emails können anhand ihrer Größe analysiert und ebenfalls abgewiesen werden. Das Limit pro Email können Sie unter der Registerkarte **Email-Größe** einstellen.

Folgende Aktionen sind bei einem Avira Email-Größenfilterung-Job möglich:

- Gesamte Email in Quarantäne stellen
- Zusatz im Betreff
- Betroffene Email löschen und nicht zustellen
- Absender oder Empfänger in Whitelist hinzufügen
- Administrator, Absender, Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Ausführen einer externen Anwendung
- Avira Tag und Wert hinzufügen
- Header Feld und Wert hinzufügen
- Email umleiten
- Header entfernen

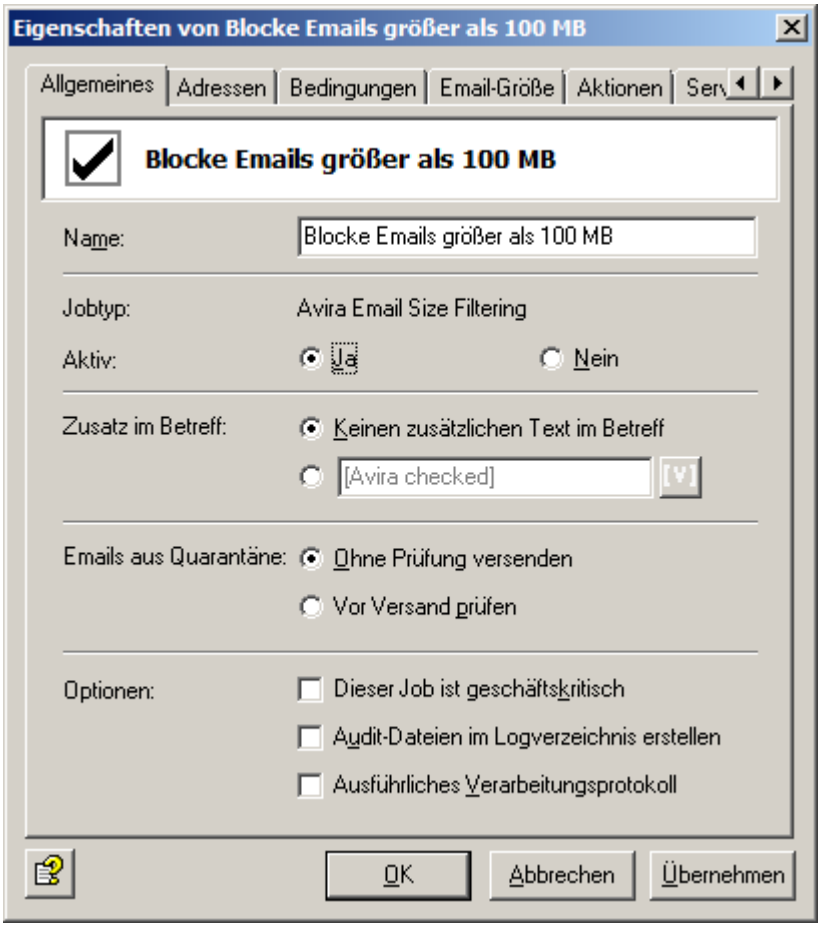
5.5.1 Email-Größe beschränken

Das folgende Beispiel basiert auf der Jobvorlage **Blocke Emails größer als 100 MB**.

Hinweis
Die Einschränkung der Email-Größe bezieht sich auf die gesamte Email inklusive Betreff, Nachrichtentext, Header und Anhang.

1. Ziehen Sie den Job per Drag-and-Drop **Blocke Emails größer als 100 MB** in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job kann auch solche Emails erneut kontrollieren, die aus der Quarantäne versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

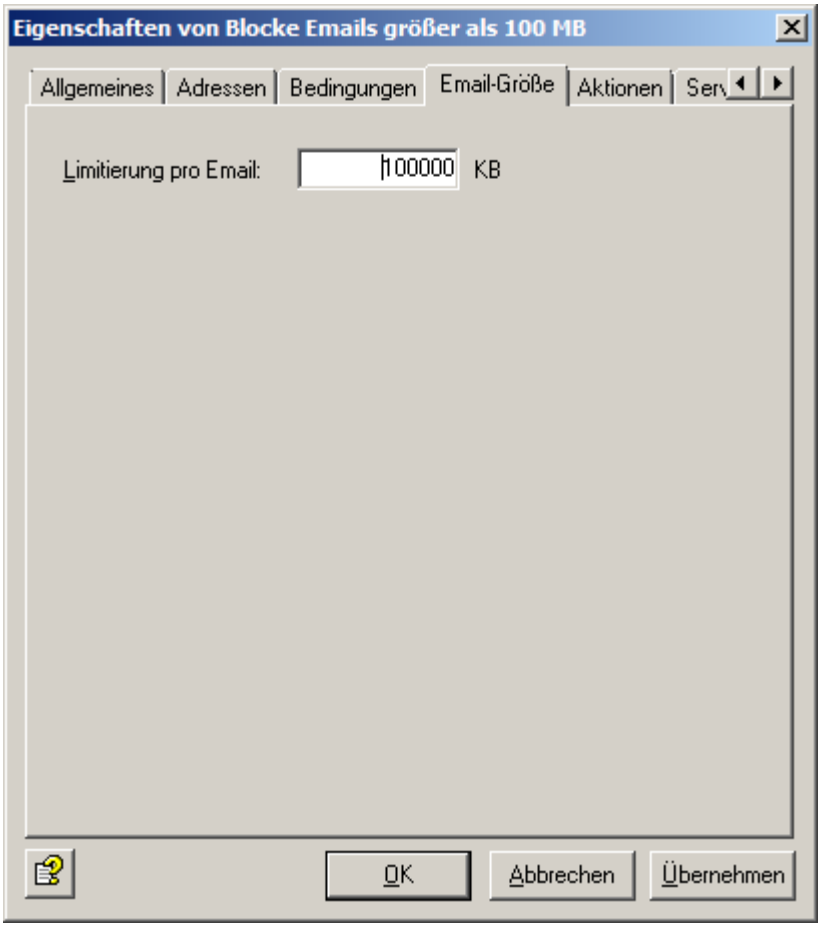
   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

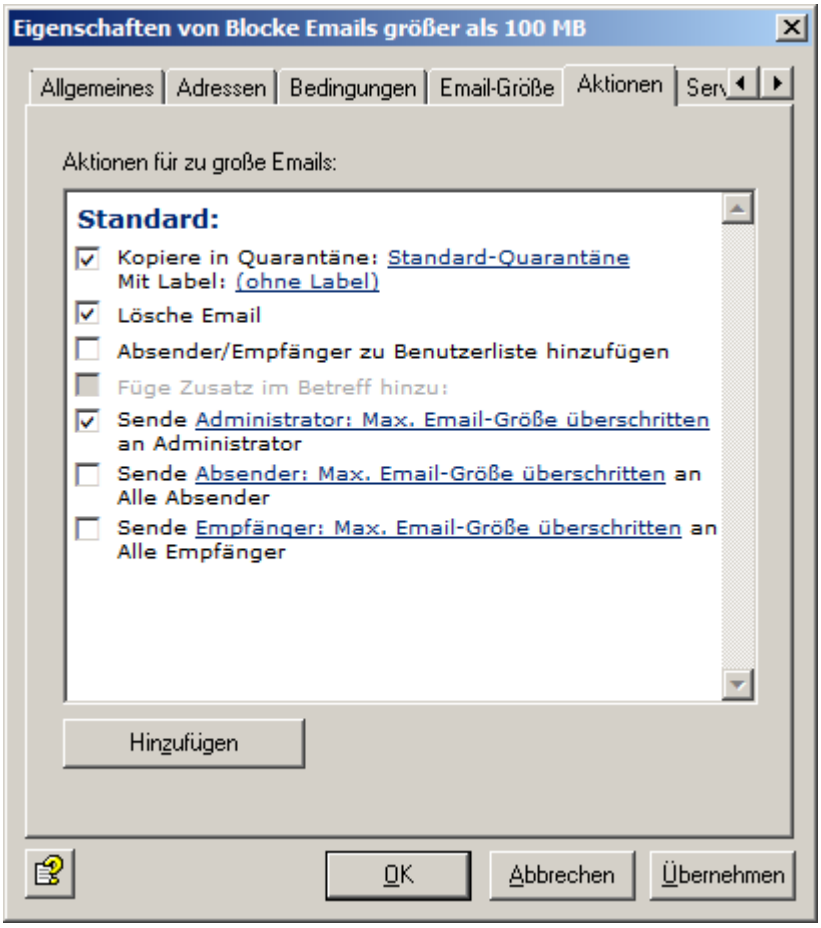
Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen in der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

6. Auf der Registerkarte `Email-Größe` geben Sie die gewünschte maximale Email-Größe in Kilobyte an.



Jede ein- und ausgehende Email darf also maximal 100.000 Kilobyte groß sein.

7. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email gefunden hat, die diese Limitierung überschreitet.



Eine Kopie der Email wird in Quarantäne verschoben und die betroffenen Anhänge werden gelöscht. Das bedeutet, dass die Email zwar an den Empfänger zugestellt wird, die verbotenen Anhänge aber entfernt werden. Eine Benachrichtigung über den gefundenen Fingerprint wird an die Administratoren versandt. Diese Benachrichtigung wird aus dem Dropdown-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

8. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
9. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

   Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
10. Auf der Registerkarte **Details** können Sie den Job näher beschreiben.
11. Klicken Sie die Schaltfläche **Konfiguration speichern** .

5.6 Avira Anhangs-/Größenfilterung Jobs

Emails können anhand der Größe ihres Anhangs analysiert und ebenfalls abgewiesen werden. Die maximale Größe eines Anhangs pro Email können Sie unter der Registerkarte **Fingerprint/Größe** einstellen. Es ist möglich, in diesem Job gleichzeitig den Typ des Anhangs einzuschränken.

Die Aktionsmöglichkeiten sind bei einem Avira Anhangs-/Größenfilterung Job dieselben wie in einem Avira Anhangsfilterung Job.

Unter **Richtlinien-Konfiguration** > **Jobvorlagen** finden Sie verschiedene Jobs für das Blockieren diverser Dateiformate und entsprechender Größen.

- **Blocke Office Dateien > 10 MB**: Microsoft Office Dateien größer als 10 MB
- **Blocke Sounddateien > 5 MB**: Sounddateien größer als 5 MB
- **Blocke Videodateien > 5 MB**: Videodateien größer 5 MB

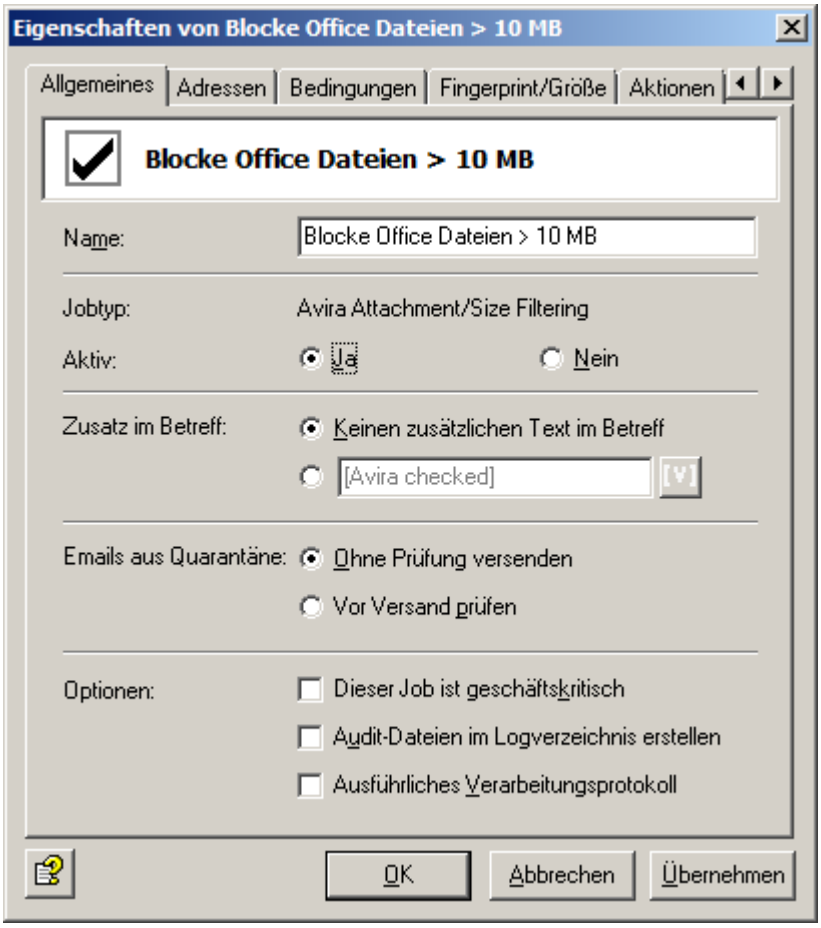
Hinweis
Die Prüfung auf Anhangformat und -größe betrifft im Gegensatz zur Prüfung der Email-Größe nur die Anhänge. Betreff, Nachrichtentext und die Kopfdaten der Email bleiben bei dieser Prüfung unberücksichtigt.

5.6.1 Office-Dateien blockieren

Als Beispiel wird hier der Job **Blocke Office-Dateien > 10 MB** behandelt.

1. Ziehen Sie den Job **Blocke Office Dateien > 10 MB** per Drag-and-Drop in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job kann auch solche Emails erneut kontrollieren, die aus der Quarantäne versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

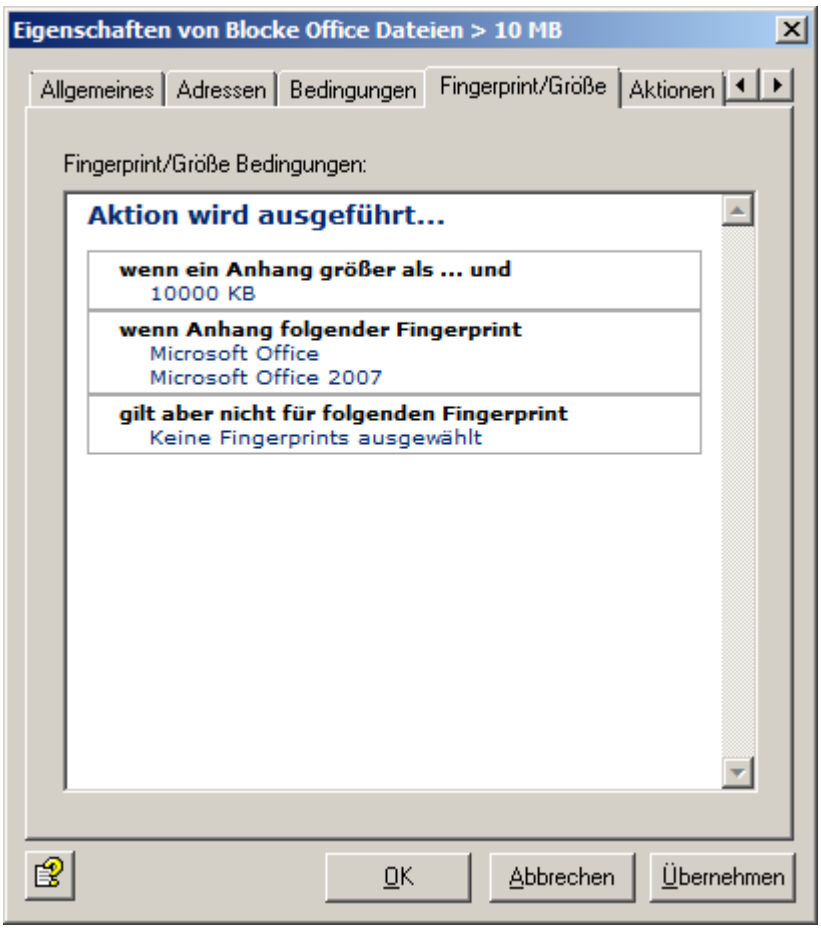
   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

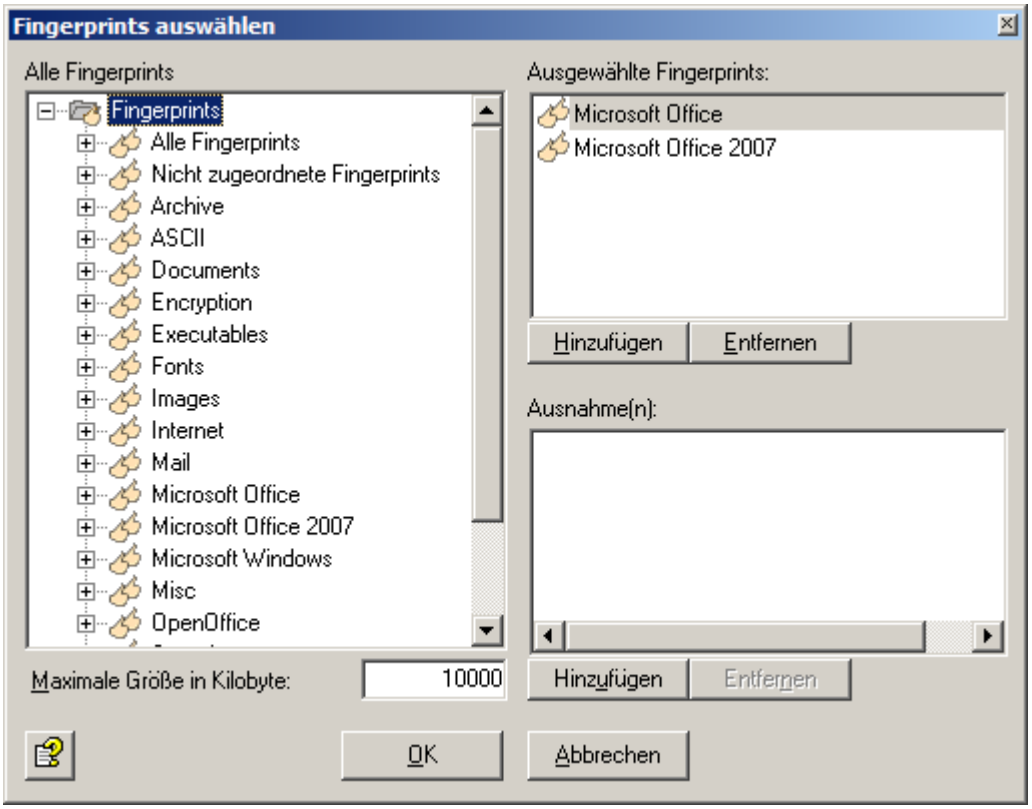
Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen in der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

6. Auf der Registerkarte **Fingerprint/Größe** geben Sie die gewünschte maximale Email-Größe und das Fingerprintformat an.



Hinweis
Im Gegensatz zur einfachen Fingerprint-Prüfung steht hier die Option zum Entpacken komprimierter Anhänge nicht zur Verfügung. Wenn Sie komprimierte Dateien in der Größe beschränken wollen, geben Sie diese Formate in diesem Job einfach an.

7. Klicken Sie auf **10.000**, um die Größe in Kilobyte festzulegen bzw. auf **Microsoft Office**, um aus der Liste der Fingerprints eine Fingerprint-Kategorie, einen einzelnen Fingerprint oder die maximale Größe zu wählen.

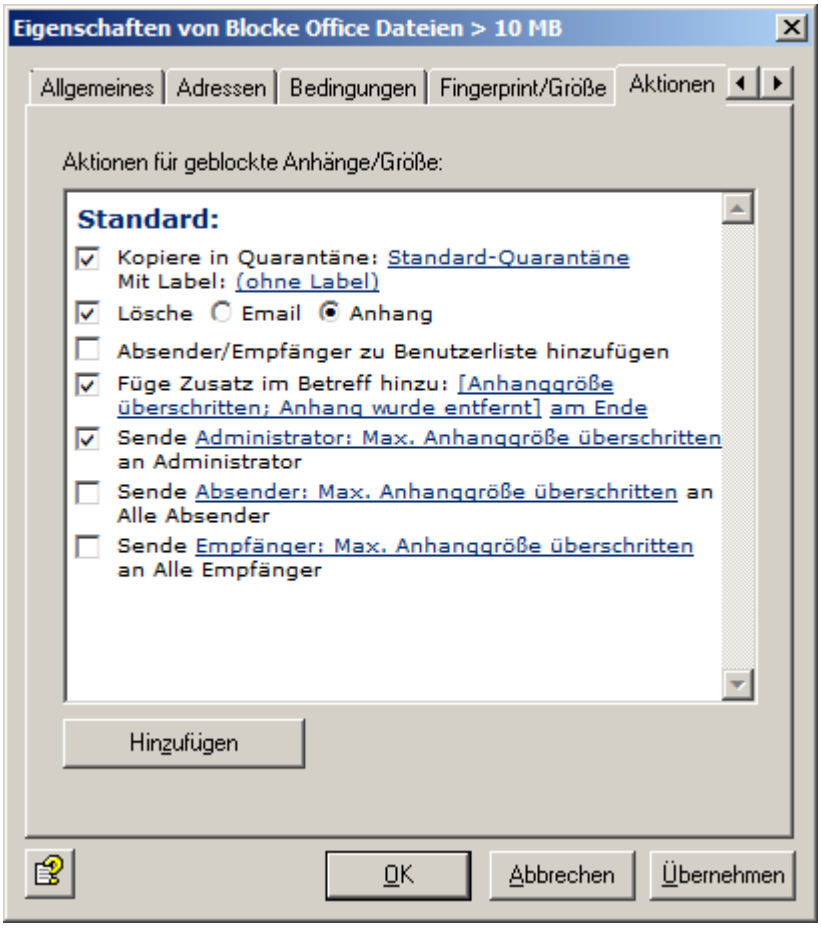


8. Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie der Liste der verbotenen und/oder erlaubten Fingerprints ganze Kategorien oder einzelne Fingerprints zuweisen. Öffnen Sie dafür die Kategorie im linken Fenster per Doppelklick oder mit einem Klick auf das **+** (Plus)-Zeichen.

Hinweis

Sie können eine Kategorie wie z. B. **Microsoft Office** unter *Ausgewählte Fingerprints* und einen einzelnen oder mehrere Fingerprint(s) dieser Kategorie unter *Ausnahme(n)* eintragen. Um eine bessere Übersicht zu behalten, sollten Sie nicht zu viele Kategorien von einem Job überprüfen lassen.

9. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email gefunden hat, die aufgrund eines Anhang/Größe-Jobs blockiert wurde.



Eine Kopie der Email wird in Quarantäne verschoben und die betroffenen Anhänge werden gelöscht. Das bedeutet, dass die Email zwar an den Empfänger zugestellt wird, die verbotenen Anhänge aber entfernt werden. Der Administrator wird über die entdeckte Restriktion informiert. Diese Benachrichtigung wird aus dem Dropdown-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

10. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
11. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

    Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
12. Auf der Registerkarte **Details** können Sie den Job näher beschreiben.
13. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Fingerprints - Seite 56

6 Avira Email-Filter

Mit Avira Email-Filter prüfen Sie den Textinhalt der Email oder der Anhänge, klassifizieren Emails nach Inhalten, beschränken Email-Adressen im Ein-/Ausgang oder limitieren die Anzahl der Empfänger pro Email.

Jobarten

- **Avira Email-Filter Adressfilterung** : Adressprüfung
- **Avira Email-Filter Inhaltsfilterung**: Prüfung der Textinhalte
- **Avira Email-Filter Empfänger-Limit-Filterung**: Prüfung der Empfängerzahl
- **Avira Filterung unerwünschter Emails** : Prüfen auf unerwünschte Email

Hinweis
Legen Sie für jeden Einschränkungstyp einen separaten Job an. Die Jobarten lassen sich später nicht mehr ändern.

Folgende Aktionen sind bei einem Avira Email-Filter-Job möglich:

- Gesamte Email in Quarantäne kopieren
- Zusatz im Betreff
- Betroffene Email löschen und nicht zustellen
- Administrator benachrichtigen
- Absender benachrichtigen
- Empfänger benachrichtigen
- Andere, frei wählbare Personen benachrichtigen
- Externe Anwendung ausführen
- Avira Tag und Wert hinzufügen
- Header-Feld und Wert hinzufügen
- Email umleiten
- Header-Feld entfernen

6.1 Adressprüfung

Die Adressprüfung konzentriert sich auf die Absender und die Empfänger einer Email. Dabei können Sie bestimmte Absender verbieten, sodass keine Email mehr von diesen zu Ihren Benutzern gelangt, oder aber auch bestimmte Empfänger, sodass keiner Ihrer Mitarbeiter (oder nur eine ausgewählte Gruppe von Mitarbeitern) an bestimmte Empfänger Emails versenden kann.

Bei der Adressprüfung können folgende Objekte verwendet werden:

- Mail-Enabled Active Directory Benutzer
- Mail-Enabled Active Directory Gruppen
- Mail-Enabled Active Directory Kontakte
- Frei definierbare SMTP Adressen, inkl. Platzhalter

- [INTERN] = Wie in Avira Exchange Security definierte interne Domänen
- [EXTERN] = Alle Adressen, die nicht [INTERN] sind
- "Administrator" = Die in Avira Exchange Security als Administrator definierten Email-Adressen

Der Eintrag in den entsprechenden Feldern der Email gibt an, ob es sich um einen Absender oder einen Empfänger handelt. Ein Absender kann also sowohl ein Mitarbeiter Ihres Unternehmens sein, der eine Email nach außen sendet, als auch eine externe Person, die einem Mitarbeiter Ihres Unternehmens eine Email schickt. Sie können sowohl Absender als auch Empfänger als Person oder als Gruppe definieren.

Bei der Adressprüfung sind folgende Platzhalter möglich:

- **Stern (*)** Der Stern symbolisiert den Platzhalter für ein oder mehrere beliebige Buchstaben und/oder Zahlen. Der Stern kann mehrfach mitten im Begriff eingesetzt werden.
- **Fragezeichen (?)** Das Fragezeichen dagegen ist der Platzhalter für ein einziges Zeichen. Auch das Fragezeichen kann mehrfach mitten im Begriff vorkommen.

Wenn Sie einen verbotenen Absender angeben, können Sie statt einzelner Email-Adressen auch `tom*@*.*` verwenden. Das heißt, dass alle Emails, die von einem Tom mit beliebiger Erweiterung (also auch Nachnamen) von welcher Domäne auch immer gesendet werden, als Absender verboten sind. Darunter fällt dann auch Ihr eigener Mitarbeiter namens Tom Jones, der somit unter die Einschränkung und dessen Emails unter die definierten Aktionen fallen.

Eine bestimmte Domäne können Sie zum Beispiel als `*@domain.com` definieren. Damit gelten alle Absender bzw. Empfänger dieser Domäne als verboten. Einen Job zur Adressprüfung mit dem Verbot einer ganzen Domäne sollten Sie nur mit großer Vorsicht serverübergreifend für alle anlegen. Es ist nicht immer klar, welche Adressen privater und welche beruflicher Natur sind. Bedenken Sie, dass kleinere Geschäftspartner durchaus Email-Adressen unter der Domäne `@tonline.de` oder `@aol.com` besitzen.

Die Adressprüfung ist ein einfaches Mittel, bekannte Adressen für unerwünschte Mails auszufiltern. Die "üblichen Verdächtigen" können vom Job auf dem Server abgefangen und sofort gelöscht werden.

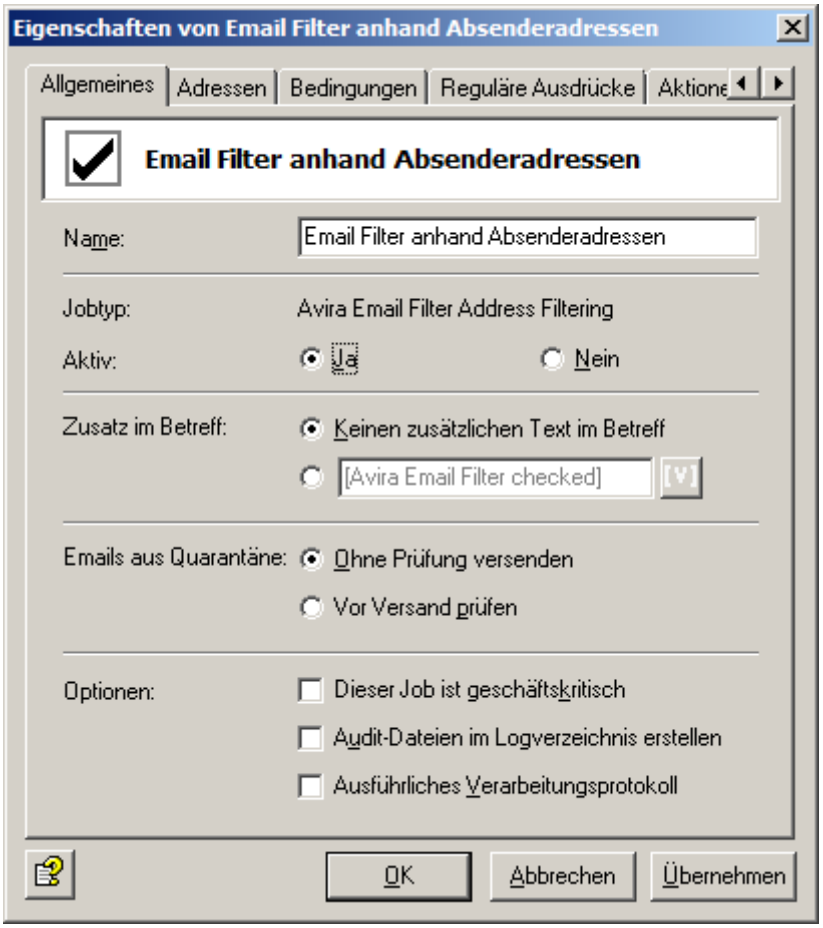
Hinweis
Im Gegensatz zu anderen Job-Arten wird bei der Adressprüfung auch dann ein ggf. konfigurierter **Zusatz im Betreff** angefügt, wenn die initiale Einschränkung nicht vorliegt. Der Grund hierfür ist, dass sich bei der Adressprüfung die initiale Einschränkung und die Jobeinschränkung entsprechen.

6.1.1 Absender oder Empfänger blockieren

Das folgende Beispiel basiert auf dem Job **Email Filter anhand Absenderadressen**.

1. Ziehen Sie den Beispieljob **Email Filter anhand Absenderadressen** in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job kann auch solche Emails kontrollieren, die aus der Quarantäne wieder versendet werden: **Vor Versand prüfen**.

Hinweis

Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

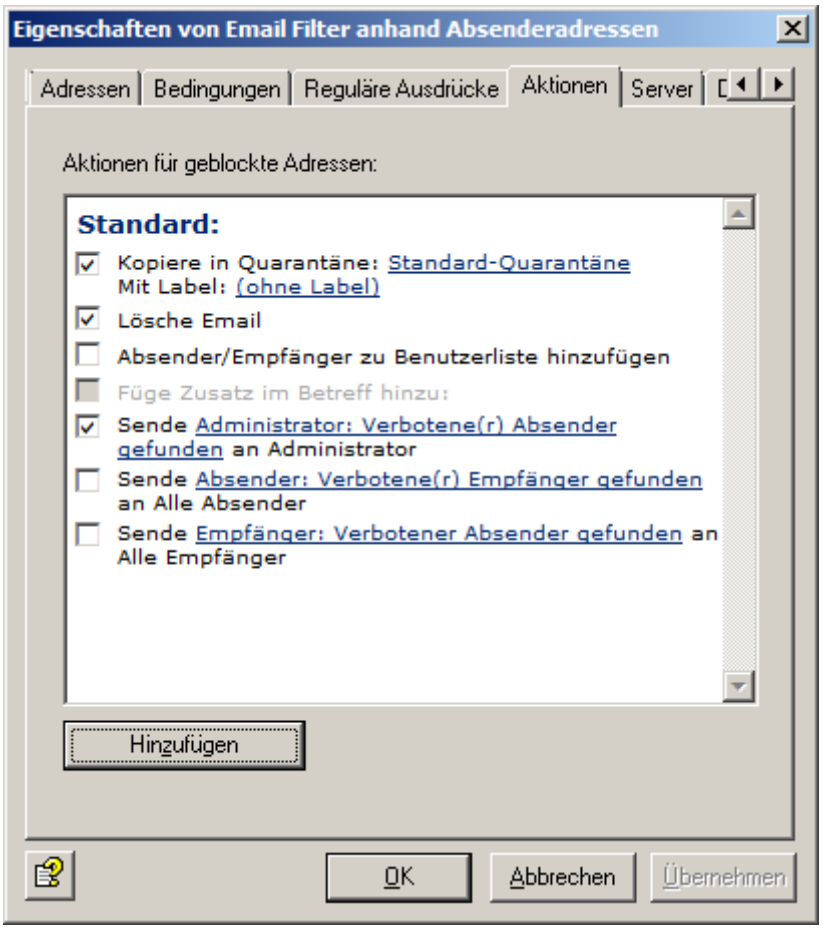
   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

6. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email mit verbotenen Adressen gefunden hat.



Eine Kopie wird in Quarantäne verschoben und die betroffene Email wird gelöscht. Das bedeutet, dass die Email nicht an den Empfänger zugestellt wird. Eine Benachrichtigung über diese Verletzung der Adressrichtlinien wird an die Administratoren versandt. Diese Benachrichtigung wird aus dem Dropdown-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

7. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
8. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

   Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
9. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Emails aus der Quarantäne senden - Seite 24
Geschäftskritische Jobs - Seite 40

Adresslisten - Seite 124
Job-Bedingungen - Seite 151
Einstellungen für einen individuellen Avira Server - Seite 111

6.2 Prüfung der Textinhalte mithilfe von Wortlisten

Avira Email-Filter verwendet vordefinierte Wortlisten, um nach unerwünschten Textinhalten zu suchen.

Folgende Bestandteile der Email können geprüft werden:

- Betreff
- Nachrichtentext
- Anhänge

Die Inhaltssuche kann auf bestimmte Absender bzw. Empfänger eingeschränkt werden. Damit können z. B. nur von außen eintreffende Emails auf Pornographie, Rassismus etc. untersucht werden.

Bei Emails von internen Absendern nach außen könnten Sie hingegen die Emails nach Firmeninterna durchsuchen lassen.

Die Emails werden anhand der zu verwendenden Wortliste durchsucht und die von Ihnen angegebenen Wörter oder Sätze innerhalb der Email gelten ab einem bestimmten Schwellwert als verboten, sobald diese Wortliste im Job aktiviert ist. Auch die Zeichenumsetzung wird im Job festgelegt. Bei erreichtem Schwellwert setzt der Job die Aktionen in Gang, die Sie vorher auf der Registerkarte **Aktionen** festgelegt haben. Zum Beispiel:

1. Die Email wird in den von Ihnen gewählten Ordner (Quarantäne) verschoben und dem Empfänger nicht zugestellt.
2. Es werden Nachrichten an Administrator, Absender und Empfänger erstellt, die die relevanten Informationen zu dem Email-Filter-Job enthalten.

Die möglichen Aktionen sind die gleichen wie bei der Adressprüfung.

Sie finden verschiedene Jobs für die Textinhaltsprüfung mit Wortlisten unter **Richtlinien-Konfiguration** › **Jobvorlagen**.

- **Blocke anstößige Inhalte** Prüfen Sie Emails auf ordinäre und pornografische Sprache.
- **Blocke Scriptkommandos** Prüfen Sie Emails auf Skript-Befehle, die Schaden anrichten können.
- **Blocke Emails mit Lebensläufen** Prüfen Sie Emails auf Begriffe aus Lebensläufen.
- **Blocke Emails von "Nigeria-Connection"** Prüfen Sie Emails auf spezielle Begriffe in "Nigeria"-Emails.

6.2.1 Wortlisten erstellen

1. Klicken Sie **Basiskonfiguration** › **Utility-Einstellungen** › **Wortlisten**.
   Um eine neue Wortliste zu erstellen, klicken Sie mit der rechten Maustaste **Wortlisten** und wählen Sie **Neu** › **Wortliste**.
2. Öffnen Sie mit einem Doppelklick eine Wortliste im rechten Fenster.

3. Vergeben Sie auf der Registerkarte **Allgemein** einen Namen für die Wortliste.
4. Geben Sie der Wortliste einen Wert von 1 bis 200.

   Dieser Wert gilt pro Wort oder Phrase und bestimmt sowohl das Verhältnis zu anderen Wortlisten als auch, wie stark die Wortliste im Job berücksichtigt wird.
5. Klicken Sie in das Eingabefeld für Wörter und fügen Sie die Wörter/ Phrasen hinzu, die Sie verbieten wollen.

   Die einzelnen Wörter/Phrasen werden mit einem Absatz (**Enter**-Taste) voneinander getrennt.

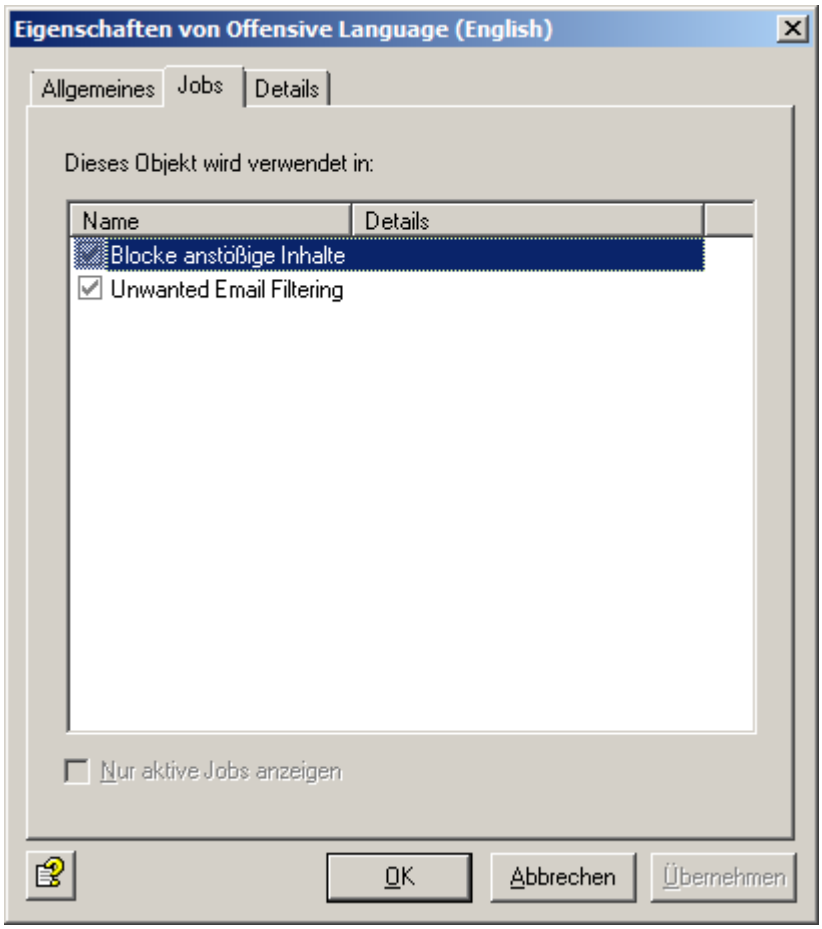
   Folgende Platzhalter sind in den Wortlisten verwendbar:

   - **Stern (*)**: Der Stern bedeutet, dass das gesuchte Wort/Phrase auch ein Teil größeren Wortes sein kann, aber nicht muss. Beispiele: `*check*` findet das einzelne Wort "check" genauso wie das Wort "checkpoint", "intercheck" oder "intercheckpoint". `check*` findet "check" genauso wie "checkpoint". Der Stern muss entweder am Anfang eines Wortes/ Phrase oder am Ende eingesetzt werden.
   - **Pluszeichen (+)**: Das Pluszeichen bedeutet das Gleiche wie der Stern mit dem Unterschied, dass das gesuchte Wort ein Teil eines größeren Wortes sein muss. Beispiele: `+check+` findet nur "checkpoint", "intercheck" oder "intercheckpoint", aber nicht "check". `check+` findet nur "checkpoint". Das Pluszeichen muss ebenfalls am Anfang oder am Ende eines Wortes/Phrase eingesetzt werden.

Hinweis
Wenn Sie weder einen Stern noch ein Pluszeichen in Ihren Wörtern/Phrasen der Wortliste einsetzen, so muss genau dieses eingegebene Wort exakt gefunden werden. Wenn Sie also `check` eingeben, so wird auch nur das einzelne Wort "check" gefunden.

6. Sortieren Sie die Wortliste nach Wunsch aufsteigend oder absteigend, indem Sie die Schaltflächen für aufsteigend und für absteigend klicken.

In welche Jobs die Wortliste eingebunden ist, ersehen Sie aus der Registerkarte **Jobs**.



Hinweis

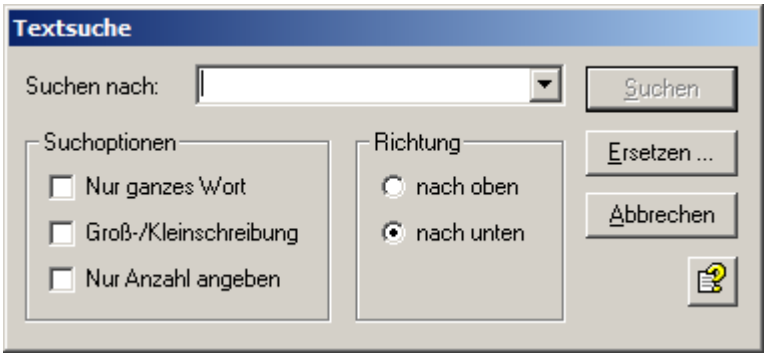
Um die Wortlisten im Job einzusetzen, wählen Sie in der Richtlinien-Konfiguration einen Content-Filtering Job aus, aktivieren die entsprechende Wortliste und bestimmen einen Gesamt-Schwellwert (von 1 bis 10.000). Sobald dieser Schwellwert durch das Addieren aller Werte (gefundene Wörter) der aktiven Wortlisten erreicht wurde, treten die definierten Aktionen in Kraft.

6.2.2 Textsuche in Wortlisten

Sie können in Wortlisten nach Begriffen suchen und sie ggf. ersetzen.

Die **Textsuche** können Sie auch für das Suchen und Ersetzen in eigenen Adressen verwenden.

1. Öffnen Sie die Wortliste mit einem Doppelklick und klicken Sie die Schaltfläche **Textsuche**

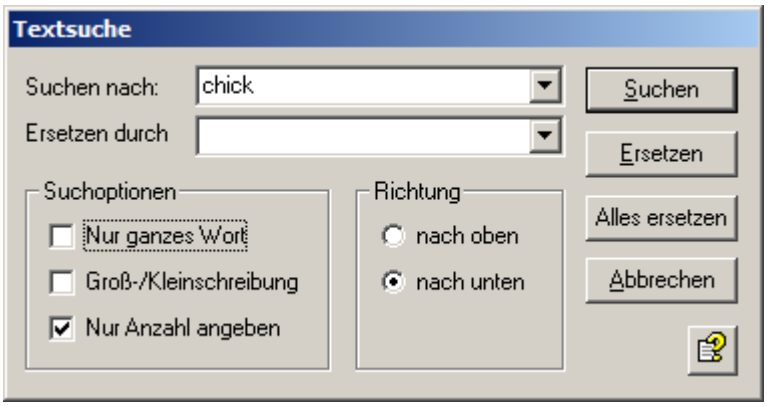


2. Geben Sie den Text ein, nach dem Sie suchen möchten und wählen Sie ggf. zusätzliche Suchoptionen.

   Wenn Sie keine Zusatzoption angeben, wird die Zeichenfolge überall gefunden, also auch in Teilen eines Wortes oder einer Phrase.

   - **Nur ganzes Wort**: Als Trennzeichen zwischen Wörtern gelten alle nicht-alphanumerischen Zeichen inklusive eines Absatz- bzw. Zeilenwechsels.
   - **Groß-/Kleinschreibung**: Berücksichtigt die Groß- und Kleinschreibung bei der Suche.
   - **Nur Anzahl angeben**: Die Treffer werden nicht direkt markiert, sondern gezählt und das Ergebnis wird als Mitteilung ausgegeben.

3. Klicken Sie die Schaltfläche **Ersetzen** und geben Sie den Text ein, den Sie als Ersatz verwenden möchten.



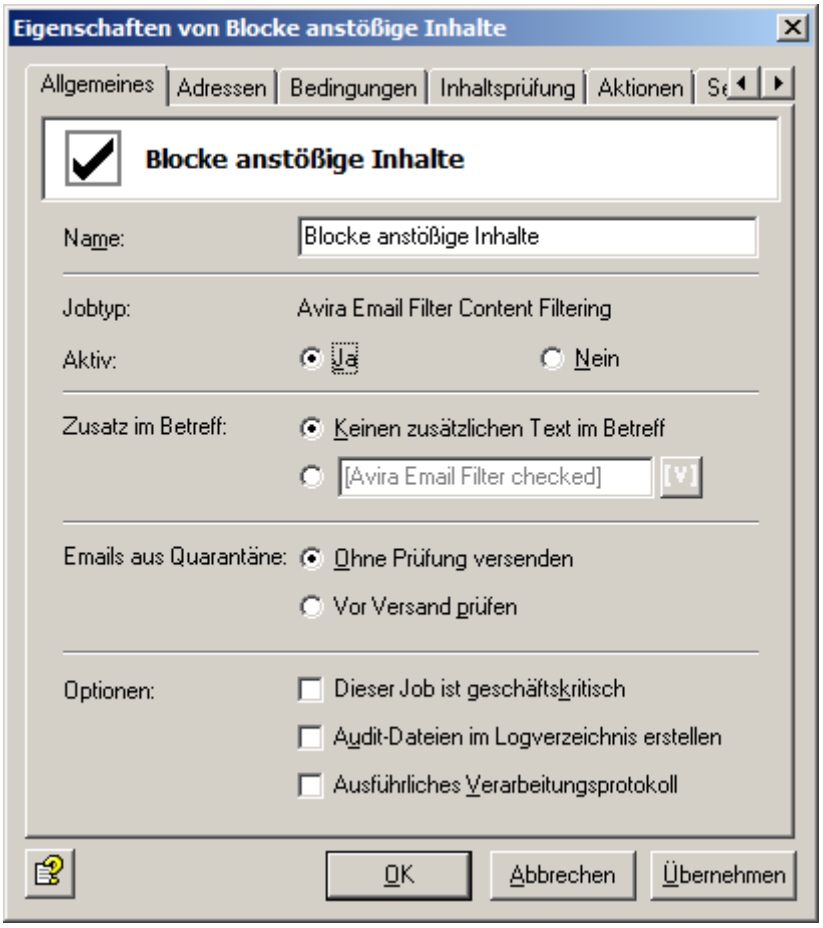
4. Klicken Sie **Suchen**, um mit der Textsuche zu beginnen.

6.2.3 Anstößige Inhalte blockieren

Als Beispiel wird hier der Job **Blocke anstößige Inhalte** behandelt.

1. Ziehen Sie den Job **Blocke anstößige Inhalte** per Drag-and-Drop in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job kann auch solche Emails kontrollieren, die aus der Quarantäne wieder versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

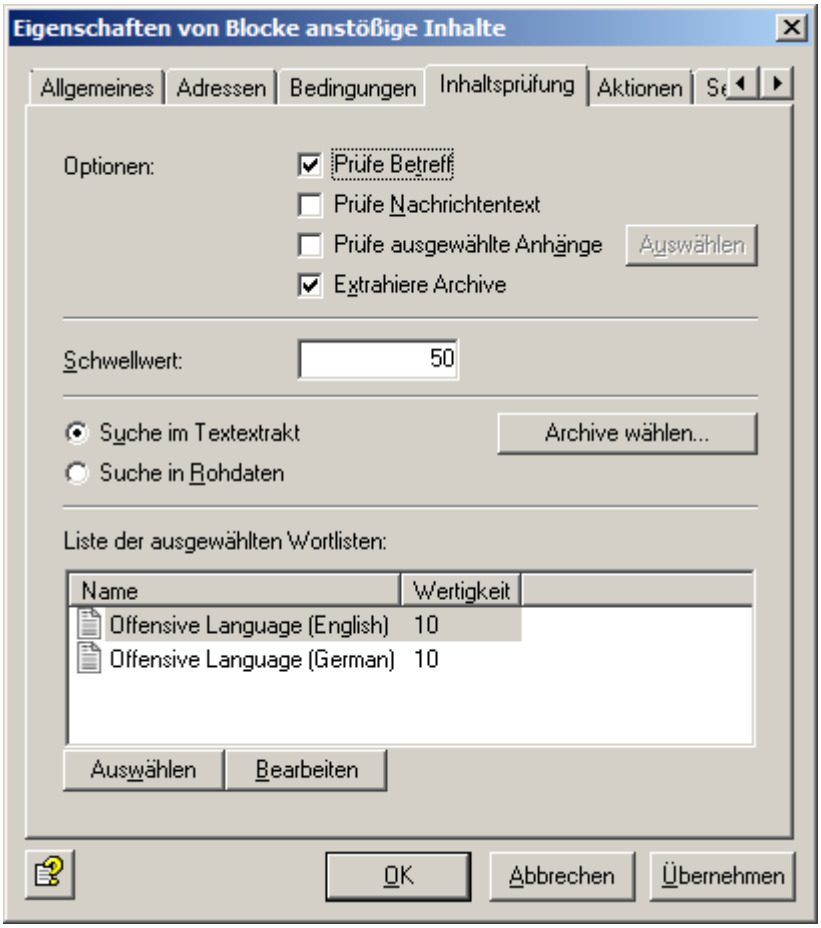
5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

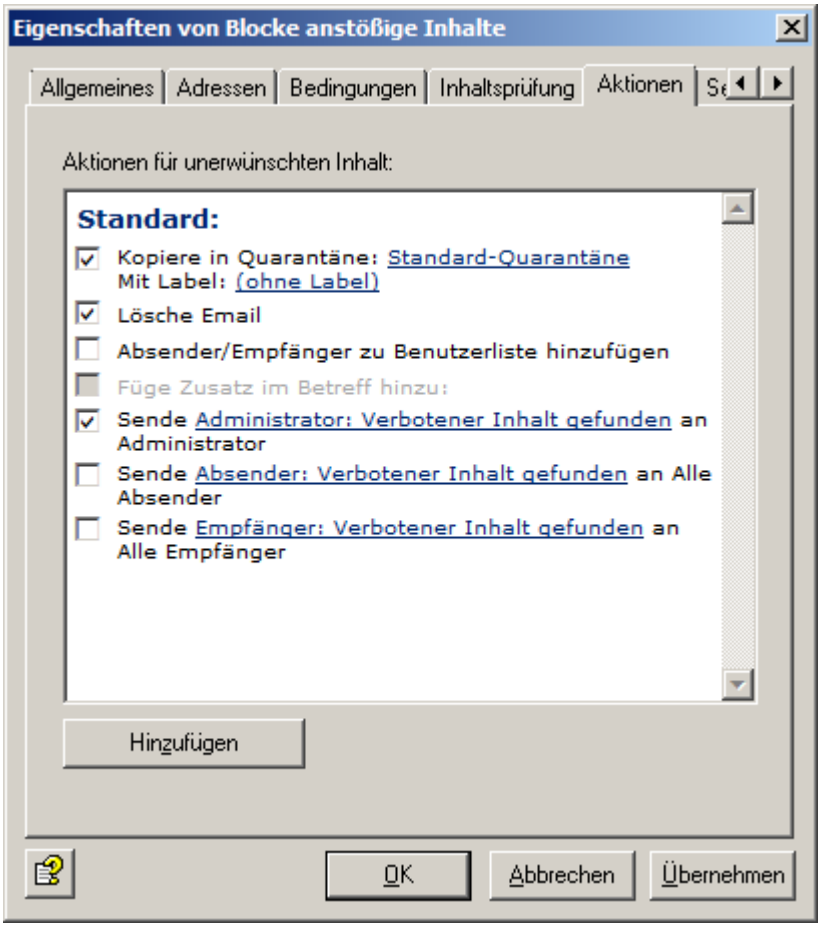
6. Wählen Sie die Wortlisten aus.

   Auf der Registerkarte **Inhaltsprüfung** stellen Sie ein, welche Wortlisten mit diesem Job aufgerufen werden sollen.



Dieser Job prüft den Betreff. Der Gesamt-Schwellwert ist auf 50 festgelegt. Damit wird bei 5 gefundenen Wörtern/Phrasen aus der Wortliste **Offensive Language (English)** oder **Offensive Language (German)** die definierten Aktionen ausgeführt.

7. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email gefunden hat, die anstößige Inhalte beinhaltet.



Eine Kopie wird in Quarantäne verschoben und die betroffene Email wird gelöscht. Das bedeutet, dass die Email nicht an den Empfänger zugestellt wird. Eine Benachrichtigung über diese Verletzung der Unternehmensrichtlinien wird an die Administratoren versandt. Diese Benachrichtigung wird aus dem Dropdown-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt. Diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

8. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
9. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Emails aus der Quarantäne senden - Seite 24
Geschäftskritische Jobs - Seite 40
Adresslisten - Seite 124
Job-Bedingungen - Seite 151
Einstellungen für einen individuellen Avira Server - Seite 111

6.2.4 Schwellwertberechnung bei Inhaltsfilterung

Unter Verwendung eines festgelegten Wertes

Rechnung: Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 10 belegt. Damit werden bei mindestens 5 gefundenen Wörtern/Phrasen aus diesen Listen die Aktionen ausgeführt.

Erklärung: Jedes Wort oder jede Phrase der Liste **Offensive Language** ist mit der Wertigkeit 10 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, die Anzahl der Wörter/Phrasen aus dieser Liste werden mit der Wertigkeit multipliziert, und die Email mit dem Schwellwert verglichen.

In diesem Beispiel also: 5 Wörter, die auf der Liste stehen, wurden in der Email gefunden. Es ergibt sich ein Wert von 5 Wörter x 10 (Wertigkeit): 5 x 10 = 50. Verglichen mit dem Schwellwert 50 = Aktion wird ausgelöst. Werden nur 4 Wörter in der Email entdeckt, beträgt der Gesamtwert nur 40 (4 x 10), der Schwellwert ist nicht erreicht und es wird keine Aktion in Gang gesetzt.

Unter Verwendung zweier Wortlisten

Sie prüfen mit zwei verschiedenen Wortlisten den Betreff und den Nachrichtentext einer Email auf verbotenen Inhalt.

Der Gesamt-Schwellwert ist im Job auf 20 festgelegt und die erste im Job angegebene Wortliste (A) hat eine Wertigkeit von 20. Die zweite in diesem Job angegebene Wortliste (B) hat eine Wertigkeit von 1. Damit werden bei 1 gefundenen Wort/Phrase aus der Wortliste A oder alternativ bei 20 gefundenen Begriffen aus der Wortliste B die definierten Aktionen ausgeführt.

Rechnung: Jedes Wort oder jede Phrase der Wortliste A ist mit der Wertigkeit 20 belegt. Damit ist bei einer einzigen gefundenen Phrase aus dieser Liste der Job-Schwellwert bereits erreicht und die Aktion wird durchgeführt.

Erklärung: Jedes Wort oder jede Phrase der Wortliste B ist mit der Wertigkeit 1 belegt. Jedes gefundene Wort/Phrase aus dieser Liste wird gezählt, die Gesamtanzahl der Wörter/Phrasen mit der Wertigkeit multipliziert und mit dem Schwellwert verglichen. Wenn hier also 21 Wörter, die auf der Liste B stehen, in der Email gefunden werden, werden diese mit der Wertigkeit 1 multipliziert: 21 x 1 = 21. Verglichen mit dem Job-Schwellwert 20 = Aktion wird ausgelöst.

Hinweis
Wenn Sie Inhalte aus verschiedenen Sprachen erkennen wollen, legen Sie die entsprechenden Wortlisten an und richten Sie pro Sprache einen Job ein. Definieren Sie bei Sprachen wie Französisch und Spanisch eine benutzerdefinierte Zeichenumsetzung. Bitte wenden Sie sich für diese Konfiguration an den Avira Support.

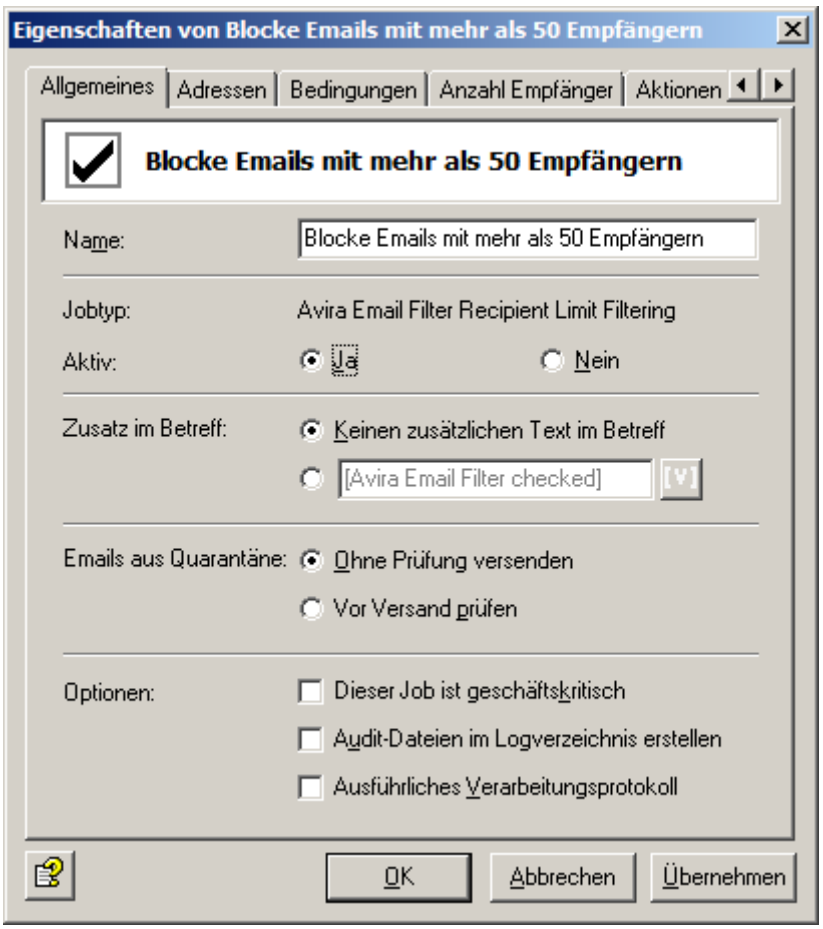
6.3 Anzahl der Empfänger einschränken

Diese Jobart ermöglicht die Begrenzung auf eine gewisse Anzahl von Empfängern pro Email. Ist dieser Job aktiv, ist es nicht möglich, unnötige Massen-Emails an alle Mitarbeiter des Unternehmens zu versenden.

Das folgende Beispiel basiert auf der Jobvorlage **Blocke Emails mit mehr als 50 Empfängern**.

1. Ziehen Sie den Job **Blocke Emails mit mehr als 50 Empfängern** per Drag-and-Drop in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.
2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere generelle Einstellungen vorzunehmen.

   Sobald Sie mit **OK** Ihre Einstellungen gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



Der **Zusatz im Betreff** ist vordefiniert auf *Avira checked*. Dieser Zusatz wird in den Betreff jeder Email eingefügt, die der Job geprüft hat.

Dieser Job kann auch solche Emails kontrollieren, die aus der Quarantäne wieder versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

4. Adressbedingungen einrichten.

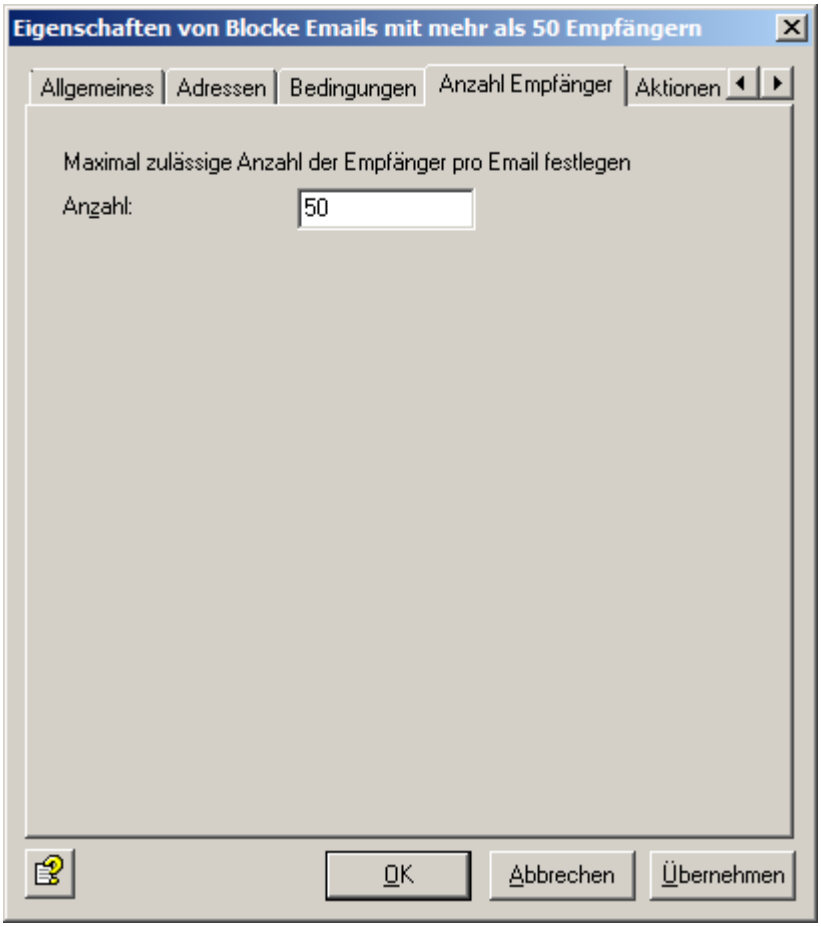
Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.

5. Inhaltliche Bedingungen einrichten.

   Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

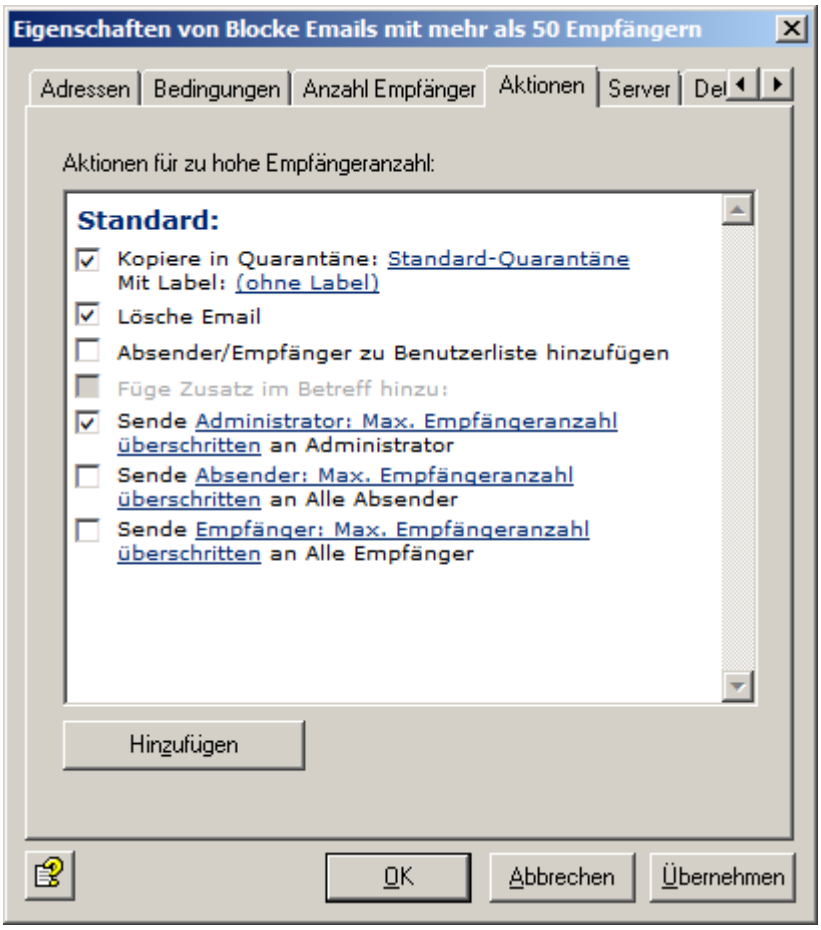
6. Auf der Registerkarte **Anzahl Empfänger** geben Sie die maximale Anzahl von Empfängern pro Email an.



in diesem Beispiel darf jede ein- und ausgehende Email an maximal 50 Empfänger adressiert sein. Sobald eine Email an 51 Empfänger adressiert ist, wird die definierte Aktion ausgelöst.

Sollten die Emails an eine Liste von Empfängern adressiert sein, die in einer einzigen Adresse zusammengefasst sind, so muss der Exchange-Server die Liste in die verschiedenen Empfänger auflösen können, um die Anzahl der Empfänger zu erkennen. Eine Adresse, die eigentlich eine Mailingliste ist, gilt als ein einziger Empfänger, wenn sie außerhalb der Reichweite des Exchange-Servers liegt.

7. Auf der Registerkarte **Aktionen** legen Sie fest, welche Aktionen durchgeführt werden sollen, wenn der Job eine Email gefunden hat, die eine gewisse Anzahl von Empfängern überschreitet.



Eine Kopie der Email wird in Quarantäne verschoben und die betroffene Email wird gelöscht. Das bedeutet, dass die Email nicht an den Empfänger zugestellt wird.
Eine Benachrichtigung über die Anzahl der Empfänger wird an die Administratoren versandt. Diese Benachrichtigung wird aus dem Dropdown-Menü der verfügbaren Benachrichtigungsvorlagen ausgewählt und diese können individuell mit der HTML-Symbolleiste oder direkt mit HTML-Formatbefehlen gestaltet werden.

8. Sie können mit der Schaltfläche **Hinzufügen** weitere Aktionen definieren.
9. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

   Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.
10. Klicken Sie die Schaltfläche **Konfiguration speichern** .

6.4 Erweiterte Email-Filter-Einstellungen

Im Email-Filter-Job lassen sich definitive und kombinierte Kriterien für unerwünschte Emails einstellen.

Die **definitiven Kriterien** bedeuten eine sofortige Entscheidung in die eine oder andere Richtung (unerwünschter oder erwünschter Inhalt) und werden sofort mit dem Etikett "Wahrscheinlichkeit für unerwünschten Inhalt ist 0 % = **Keine**" oder "Wahrscheinlichkeit für unerwünschten Inhalt ist 100 % = **Hoch**" belegt.

Die **kombinierten Kriterien** werden nur dann angewandt, wenn die definitiven Kriterien nicht zutreffend waren. Für die eigentliche Erkennung von unerwünschtem Inhalt mit kombinierten Kriterien werden mehrere Analyse-Mechanismen (Kriterien-Untersuchungen) parallel durchgeführt und anschließend nach der Analyse der Email miteinander "verrechnet".

Deaktiviert wird das Kriterium mit Klick in die Checkbox.

Jedes Kriterium besitzt seine eigene Relevanz für das Gesamtergebnis (die individuelle Wertigkeit dieses Kriteriums), die von **Niedrig** bis **Sehr hoch** eingestellt werden kann.

Außerdem lassen sich die meisten Kriterien noch mit einem individuellen Wert für **Minimum** und **Maximum** belegen. Diese beiden Werte beziehen sich z. B. auf die Wortlisten, gegen die das Kriterium die Emails prüft. Unterhalb des Minimum-Werts wird dieses Kriterium für die entsprechende Email in der Gesamtwertung nicht berücksichtigt. Ist der Maximum-Wert erreicht, so ist dieses Kriterium der Meinung: "*Dies ist unerwünschter Inhalt!*"

Warnung
Die Aussage "*Dies ist unerwünschter Inhalt!*" gilt nur für das konkrete einzelne Kriterium, dessen Maximum-Wert durch die Analyse der Email erreicht ist. Da es sich bei dieser Analyse auf unerwünschten Inhalt immer um eine Analyse mit kombinierten Kriterien handelt, können die anderen Kriterien auch "anderer Meinung sein" und beim gegenseitigen Verrechnen das einzelne Kriterium sozusagen "überstimmen".

6.4.1 Definitive Kriterien

Wichtig für eine gute Email-Lösung ist auch die effektive Vermeidung falsch klassifizierter Emails (*False Positives*) und die effiziente Verwendung der für die Inhaltsprüfung zur Verfügung stehenden Rechenleistung im Produktivbetrieb. Aus diesem Grund sind die **definitiven Ausschlusskriterien** (= definitive Kriterien) den kombinierten Kriterien vorangestellt, sodass keine weiteren Inhaltsprüfungen bei Emails vorgenommen werden müssen, wenn die definitiven Kriterien erfüllt sind. Die Ausschlusskriterien werden verwendet, um die Prüfungen auf unerwünschten Inhalt auf diejenigen Emails zu beschränken, die (beispielsweise aufgrund des Absenders) noch nicht als unerwünschte Emails ausgeschlossen werden können.

Definitive Kriterien für erwünschte Emails

Im Job können die folgenden Kriterien konfiguriert werden, aufgrund derer Emails automatisch als nicht bedrohlich oder als erwünscht angesehen werden:

Kriterium	Beschreibung
Emails der folgenden Absender (Whitelist)	Whitelist: Adressen aller bekannten Absender, die immer erlaubt sind und die eindeutig keinen unerwünschten Inhalt versenden. Dies sind im Prinzip alle regelmäßigen Kommunikationspartner und die Domänen von Kunden und Lieferanten. Je vollständiger diese Liste gehalten wird, desto weniger wird Ihr System mit unnötigen Prüfungen belastet.
Emails von Active Directory Benutzern	Weitere vertrauenswürdige Adressen sind alle im Active Directory eingetragenen Benutzer und Kontakte.
Emails von Absendern in Benutzer-Whitelist	Die in der Benutzer-Whitelist eingetragenen Email-Adressen werden ohne Prüfung auf unerwünschten Inhalt durchgelassen.
Emails mit Anhängen	Emails mit Dateianhängen. Die meisten unerwünschten Emails enthalten keine Anhänge. Optional können Sie hier einen Schwellwert eintragen. Beispiel: Mindestwert = 2, d. h. alle Emails, die nur zwei Anhänge haben, werden ohne Prüfung auf unerwünschten Inhalt zugestellt.
Emails mit Mindestgröße (in Kilobyte)	Unerwünschte Emails sind in der Regel klein. Deshalb handelt es sich bei großen Emails meist nicht um unerwünschte Emails. Hier kann ein Schwellwert eingestellt werden, ab dem größere Emails nicht mehr auf unerwünschten Inhalt geprüft werden.
Emails sind in TNEF-Format	TNEF-Emails. Dieses Exchange-spezifische Format wird bisher nicht von Spammern benutzt.
Emails sind verschlüsselt oder signiert	Verschlüsselte und/oder signierte Emails. Spammer versenden bisher keine verschlüsselten oder signierten Emails.
Microsoft Exchange "Kein Spam" SCL-Wert	Spam Confidence Level (SCL), Spam-Filter (Intelligent Message Filter (IMF)) ab Exchange 2003. SCL kann ganze Zahlen zwischen -1 und 9 annehmen. -1 wird von

Kriterium	Beschreibung
	Exchange für Emails von Absendern aus der gleichen Exchange-Organisation vergeben. Dieser Wert wird vom Email-Filter-Job zur Prüfung auf unerwünschte Inhalte als definitives "Kein Spam"-Kriterium gewertet.

Verwandte Themen:

Ergebnis für unerwünschten Inhalt in Exchange-SCL-Feld schreiben - Seite 99

Definitive Kriterien für unerwünschte Email

Damit eine Email auf jeden Fall gefiltert und gegebenenfalls abgefangen wird, können folgende Ausschlusskriterien definiert werden.

Kriterium	Beschreibung
Emails der folgenden Absender (Blacklist)	Blacklist: Adressen aller Absender, die immer als unerwünschte Absender identifiziert werden. Die Standardkonfiguration enthält bereits eine Liste bekannter Adressen. Sie können zusätzlich eigene Adressen definieren.
Emails von Absendern in Benutzer Blacklist	Die in der Benutzer-Blacklist eingetragenen Email-Adressen werden ohne Prüfung auf unerwünschten Inhalt blockiert.
Emails mit diesem Zeichensatz	Die Funktion prüft das Feld "charset" in den Kopfzeilen (Header) der Email auf die Zeichensätze, die in der angegebenen Liste eingetragen sind. Emails mit einem solchen Zeichensatz werden sofort als unerwünscht klassifiziert.
Exchange SenderID-Ergebnis = "FAIL"	Wenn Sie dieses Kriterium aktivieren, wird die Sender-ID der Email mit ausgewertet. Dadurch wird "Spoofing", also das Fälschen von Absender-Email-Adress-Domains, verhindert. Die Auswertung erfolgt anhand von Einträgen in einem DNS. Über dieses DNS kann ermittelt werden, von welchen IP-Adressen Emails bestimmter Domains versandt bzw. nicht versandt werden dürfen. Das Ergebnis der Sender-ID wird mit der Email mitgeliefert. Email-Filter prüft die Sender-ID der Email und

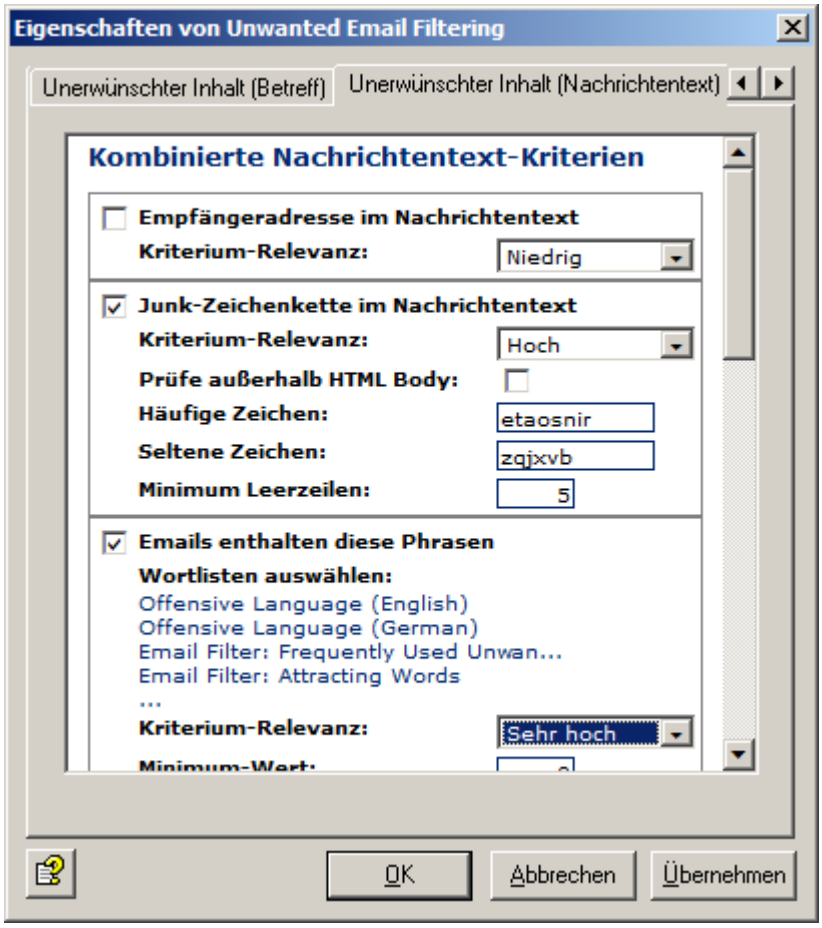
Kriterium	Beschreibung
	wertet das Ergebnis "FAIL" als unerwünscht aus. Um die Funktion SenderID nutzen zu können, müssen Sie einige Funktionen am Server aktivieren, z. B. die zugehörigen Filter für SenderID am Server. Die Aktivierung erfolgt unter **Server** > **Protokolle** > **SMTP** > **Eigenschaften** im Feld **Identifikation**. Darüber hinaus müssen sowohl Server als auch Client (Outlook) konfiguriert werden. Siehe *Details:SenderID*.
GTUBE Testmuster	Diese Funktion überprüft Emails auf das GTUBE Testmuster.

Sollen Emails nur dann direkt gelöscht werden, wenn diese definitiv unerwünscht sind, müssen Sie die Email-Filter-Wahrscheinlichkeit für **Hoch** auf 100 setzen und eine entsprechende Aktion definieren. Dadurch wird sichergestellt, dass nur die Emails, bei denen anhand der definitiven Kriterien (= die Blacklist des Zeichensatzes) eindeutig "unerwünscht" festgestellt wurde, in diesen Bereich fallen. Bei einer Einstellung zwischen z. B. 91 und 100 fallen auch Emails mit einer hohen Wahrscheinlichkeit für unerwünschten Inhalt aus anderen Kriterien in diesen Bereich.

6.4.2 Kombinierte Kriterien

Einige der kombinierten Kriterien liegen häufig bei unerwünschtem Inhalt in der "Grauzone" vor. Jedes der kombinierten Kriterien ist normalerweise für sich genommen lediglich ein Hinweis darauf, ob eine Email bestimmte Merkmale für unerwünschten Inhalt aufweist. Je mehr Kriterien mit einem hohen Wert für unerwünschten Inhalt eine Email erfüllt, desto wahrscheinlicher ist es, dass es sich in der Tat um eine Email mit unerwünschtem Inhalt handelt. Die Kombination der einzelnen Ergebnisse dieser Kriterien (d. h. die "kombinierten Kriterien") ergibt einen Messwert im Job, der den Wahrscheinlichkeitsgrad dafür bestimmt, dass es sich bei dieser Email um unerwünschten Inhalt handelt (= Wahrscheinlichkeit für unerwünschten Inhalt).

Beispiel für kombinierte Kriterien



Im kombinierten Kriterium **Emails enthalten diese Phrasen** auf der Registerkarte **Unerwünschte Mail (Nachrichtentext)** verwenden Sie u. a. die Wortliste **Email-Filter: Häufig verwendete unerwünschte Phrasen**, um den Nachrichtentext aller eingehenden Emails auf unerwünschten Inhalt zu prüfen. Diese Wortliste wird auf eine Wertigkeit von 5 gesetzt. Wenn ein Wort bzw. eine Phrase aus dieser Wortliste, beispielsweise "*testen Sie es*", in einer Email gefunden wird, wird dieses Wort bzw. diese Phrase bewertet und erhält den Zähler 5. Anschließend geben Sie die Gesamtzahl der Wörter an, aus denen dieses Kriterium in der Gesamtwertigkeit (**Minimum**) berücksichtigt werden soll, und wann Ihr individueller "Messwert für unerwünschte Email" (**Maximum**) für dieses Kriterium voll ist. Hierzu addieren Sie die Wertigkeiten der zu findenden Wörter. Wenn Sie hier einen Wert von 30 angeben (wie in Ihrem vorkonfigurierten Job), müssen sechs verschiedene Wörter aus der Wortliste in der Email gefunden werden, damit die Email vollständig für dieses Kriterium als unerwünschte Email klassifiziert wird (die Wertigkeit der Wortliste und der in ihr enthaltenen Wörter beträgt 5). Wenn hier beispielsweise nur drei verschiedene Wörter gefunden werden, ist diese Email für dieses Kriterium nicht "vollständig" unerwünscht, aber die Wahrscheinlichkeit dafür ist ziemlich hoch. Bei einer anderen Wortliste mit der Wertigkeit von 10 würden drei Treffer natürlich für den Hinweis "vollständig" unerwünschte Email ausreichen.

Mehrere gleiche Wörter werden nicht mehrfach, sondern nur einmal gezählt. Sollte also in diesem Beispiel in der Email dreimal der Begriff "*testen Sie es*" vorkommen, so zählt dieser Begriff insgesamt nur mit dem Wert 5 und nicht mit dem Wert 15 (im Gegensatz zu einem normalen Job Avira Email-Filter Inhaltsfilterung).

Zusätzlich geben Sie die **Kriterium-Relevanz** an. Wenn Sie diese auf **Sehr hoch** eingestellt haben, wird das Kriterium in der Gesamtwertung entsprechend stark berücksichtigt.

Kombination der Hinweise zur Wahrscheinlichkeit unerwünschten Inhalts

Die Einzelwertigkeiten aller kombinierten Kriterien werden anschließend entsprechend ihrer eingestellten Relevanz gewichtet, und es wird eine Gesamtwertigkeit errechnet. Der Job vergleicht diese Gesamtwertigkeit (= Wahrscheinlichkeit für unerwünschten Inhalt in der Email) am Ende der Prüfung mit den drei einzeln festzusetzenden Schwellwerten und weist die Email einem der vier Wahrscheinlichkeitsbereiche für unerwünschten Inhalt zu (**Keine** bis **Hoch**). Zusammen mit anderen kombinierten Kriterien kann unsere Beispielmail mit den drei gefundenen Wörtern der Wortliste mit einer Wertigkeit von 5 daher noch immer in der Gesamtberechnung unter die Kategorie "unerwünschter Inhalt" fallen.

In diesem Beispiel könnte unsere Email mit den sechs gefundenen Wörtern der Wortliste mit der Wertigkeit 5, die in diesem Kriterium den Stempel "Das ist vollständig unerwünschter Inhalt“ erhalten hat, durch die Aufrechnung mit anderen Kriterien auch die Wahrscheinlichkeit für unerwünschten Inhalt **Keine** oder **Niedrig** und damit am Ende im Gesamtergebnis den Stempel "Das ist wahrscheinlich kein unerwünschter Inhalt" erhalten haben.

Die Gesamtwertung resultiert erst aus den Kriterium-Relevanzen, den Minimum- und Maximum-Werten und der individuell eingestellten Email.

Die einzelnen kombinierten Kriterien finden Sie unter **Erweiterte Konfiguration** auf vier Registerkarten.

Bitte wenden Sie sich für weiterführende Informationen zu kombinierten Kriterien an den Avira-Support.

Kombiniertes Kein unerwünschter Inhalt-Kriterium

Kriterium	Beschreibung
Emails enthalten diese Phrasen	Überprüft, ob sich Wörter aus dem typischen Business-Wortschatz der Anwender im Nachrichtentext der Email befinden.

Kombinierte Klassifizierungskriterien

Hier werden Ergebnisse von anderen Produkten zur Erkennung unerwünschter Inhalte eingerechnet, von denen jedes oft als alleiniges Erkennungsmerkmal für unerwünschte Inhalte eingesetzt wird. Durch die Kombination mit anderen Kriterien im Avira Filterung unerwünschter Emails -Job werden die spezifischen Nachteile der einzelnen Produkte kompensiert.

Kriterium	Beschreibung
Exchange SCL Wert	Der Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob es sich bei einer Email um unerwünschten Inhalt handelt. Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganze Zahlen zwischen -1 und 9 annehmen. Je höher der SCL, desto größer ist auch die Wahrscheinlichkeit für unerwünschten Inhalt. Der SCL-Wert einer Email kann über dieses Kriterium in die Bewertung von Avira Email-Filter einbezogen werden. Für weitere Informationen siehe auch *http://technet.microsoft.com/en-us/library/bb124426%28v=EXCHG.65%29.aspx*.

Verwandte Themen:

Definitive Kriterien für erwünschte Emails - Seite 85

Ergebnis für unerwünschten Inhalt in Exchange-SCL-Feld schreiben - Seite 99

Kombinierte Header-Kriterien

Kriterium	Beschreibung
Suspekte Absendereigenschaften	Überprüft, ob der "From"-Header vorhanden und gefüllt ist und ob er mit dem Absender des SMTP-Protokolls übereinstimmt.
Suspekte Empfängereigenschaften	Überprüft, ob der "To"-Header und ein Eintrag vorhanden sind und ob sich mindestens einer der SMTP-Empfänger im "To"- oder "CC"-Header befindet.
Zahlen in Absenderadresse(n)	Überprüft, ob sich in einer der Absender-Adressen (SMTP oder Email-Header) Ziffern befinden.
Anzahl Empfänger pro Email	Überprüft die Anzahl der Empfänger einer Email.
Bekannter X-Mailer	Überprüft, ob es sich beim X-Mailer-Eintrag in der Email um einen bekannten Client für unerwünschten Inhalt handelt.
Bekannte Ergebnisse für unerwünschten Inhalt	Berücksichtigt das Ergebnis einer vorgeschalteten Inhaltsanalyse zur

Kriterium	Beschreibung
	Klassifizierung von Emails als unerwünschter bzw. nicht unerwünschter Inhalt. Das Ergebnis (Anzahl der gefundenen Hinweise auf unerwünschten Inhalt) wird in den X-Header der Email geschrieben. Avira Exchange Security wertet den X-Header aus und schreibt die Anzahl der Hinweise auf unerwünschten Inhalt in das Kriterium. Anhand der Angaben über die minimale bzw. maximale Anzahl an möglichen Hinweisen auf unerwünschten Inhalt erfolgt die Auswertung. Das Ergebnis kann von einem externen System stammen oder von Avira Exchange Security eines anderen Servers ermittelt worden sein.

Kombinierte Betreff-Kriterien

Kriterium	Beschreibung
Fehlender Betreff	Überprüft, ob das Betreff-Feld und ein Eintrag vorhanden sind.
Empfängeradresse im Betreff	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Betreff der Email befindet.
Junk-Zeichenkette im Betreff	Überprüft, ob lange Zeichenketten von versteckten Zeichen (Leerzeichen) und sinnlose Junk-Zeichenketten im Betreff der Email vorkommen.
Emails enthalten diese Phrasen	Überprüft, ob sich Wörter aus dem typischen Spam-Wortschatz im Betreff der Email befinden.
Emails enthalten diese verschleierten Wörter	Fehlender Betreff

Kombinierte Nachrichten-Kriterien

Kriterium	Beschreibung
Empfängeradresse im Nachrichtentext	Überprüft, ob sich der Teil vor dem @ einer Empfänger-Adresse im Nachrichtentext der Email befindet.

Kriterium	Beschreibung
Junk-Zeichenkette im Nachrichtentext	Überprüft, ob lange Zeichenketten von versteckten Zeichen und sinnlose Junk-Zeichenketten im Nachrichtentext der Email vorkommen.
Emails enthalten diese Phrasen	Überprüft, ob sich Wörter aus dem typischen Wortschatz für unerwünschten Inhalt im Nachrichtentext der Email befinden.
Emails enthalten diese verschleierten Wörter	Überprüft, ob sich verschleierte Wörter aus der/den angegebenen Wortliste(n) im Nachrichtentext der Email befinden.
Emails enthalten suspekten HTML-Code	Überprüft, ob sich HTML-Konstrukte im Nachrichtentext der Email befinden.
Emails enthalten suspekte HTML-Links	Überprüft, ob sich unerwünschte Links im Nachrichtentext der Email befinden.
Viele HTML-Links	Überprüft, ob sich im Verhältnis zum Textumfang viele HTML-Links im Nachrichtentext der Email befinden.
Eingebettete Bilder	Überprüft, ob unerwünschter Inhalt vorhanden ist, der durch eingebettete Bilder transportiert werden kann (interner Verweis auf Anhänge). Beispielsweise ist es so möglich, dass in Konfigurationen ohne Avira Email-Filter Emails mit eingebetteten Bildern pauschal als unerwünschter Inhalt bewertet werden, sofern eingebettete Bilder nicht auch Bestandteil der regulären Email-Kommunikation der Einsatzumgebung sind.

6.4.3 Erweiterte Email-Filterung

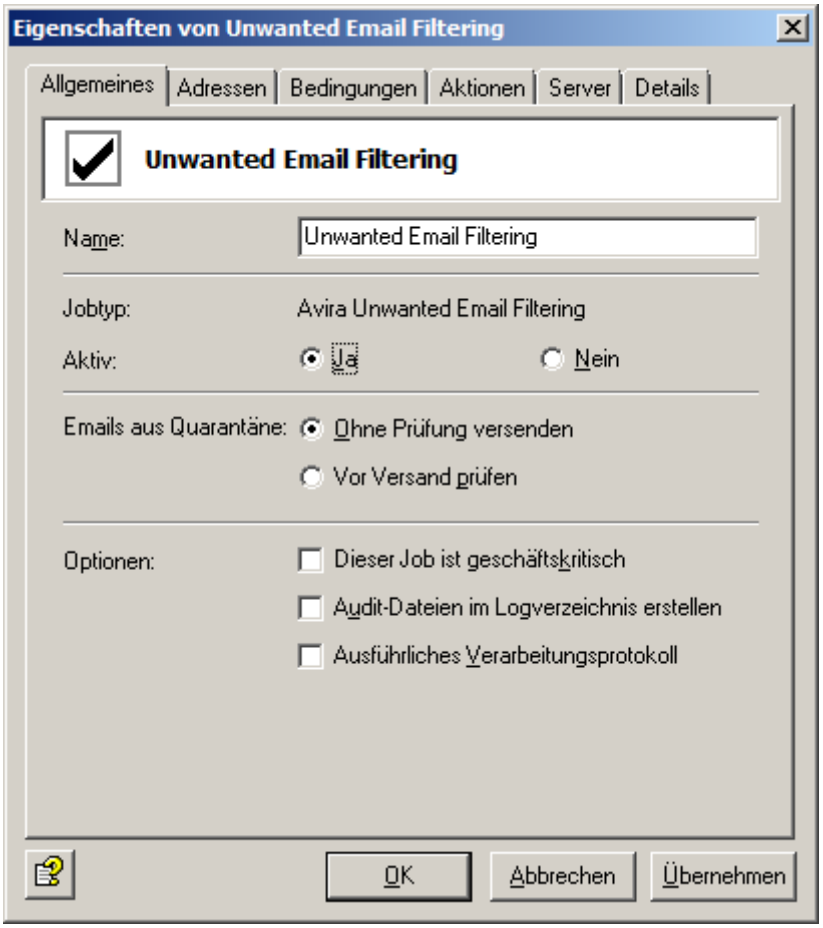
Warnung
Für Ihre Sicherheit wurde der Job **Filterung unerwünschten Inhalts mit Avira Email-Filter** vorkonfiguriert und voraktiviert. Sie finden den Job unter **Mail-Transport-Jobs**.

Sie können auch den Job **Erweiterte Email-Filterung** verwenden, der Emails anhand spezieller Email-Filteranweisungen untersucht.

1. Ziehen Sie den Job **Erweiterte Email-Filterung** in den Ordner **Mail-Transport-Jobs** und öffnen Sie ihn dort mit einem Doppelklick.

2. Auf der Registerkarte **Allgemeines** können Sie einen Namen für den Job vergeben.
3. Klicken Sie **Ja**, um den Job zu aktivieren und weitere allgemeine Einstellungen vorzunehmen.

   Sobald Sie Ihre Einstellungen mit **OK** gespeichert und den Job geschlossen haben, ist der Job aktiviert. Dass der Job aktiv ist, erkennen Sie sofort an dem Haken im Job-Symbol.



   In diesem Job ist der **Zusatz im Betreff** auf der Registerkarte **Aktionen** zu finden.

   Dieser Job kann auch solche Emails kontrollieren, die aus der Quarantäne wieder versendet werden: **Vor Versand prüfen**.

Hinweis
Die Sende-Option beim **Versand aus der Quarantäne** ist jobübergreifend und hat Priorität. Wenn Sie eine Email also mit der Quarantäne-Sende-Option **Zustellen ohne weitere Avira Prüfung dieses Servers** erneut versenden, wird die Mail durch keinen Job bearbeitet. Setzen Sie beim Versand aus der Quarantäne die Sende-Option deshalb auf **Email erneut durch Avira Jobs dieses Servers bearbeiten**.

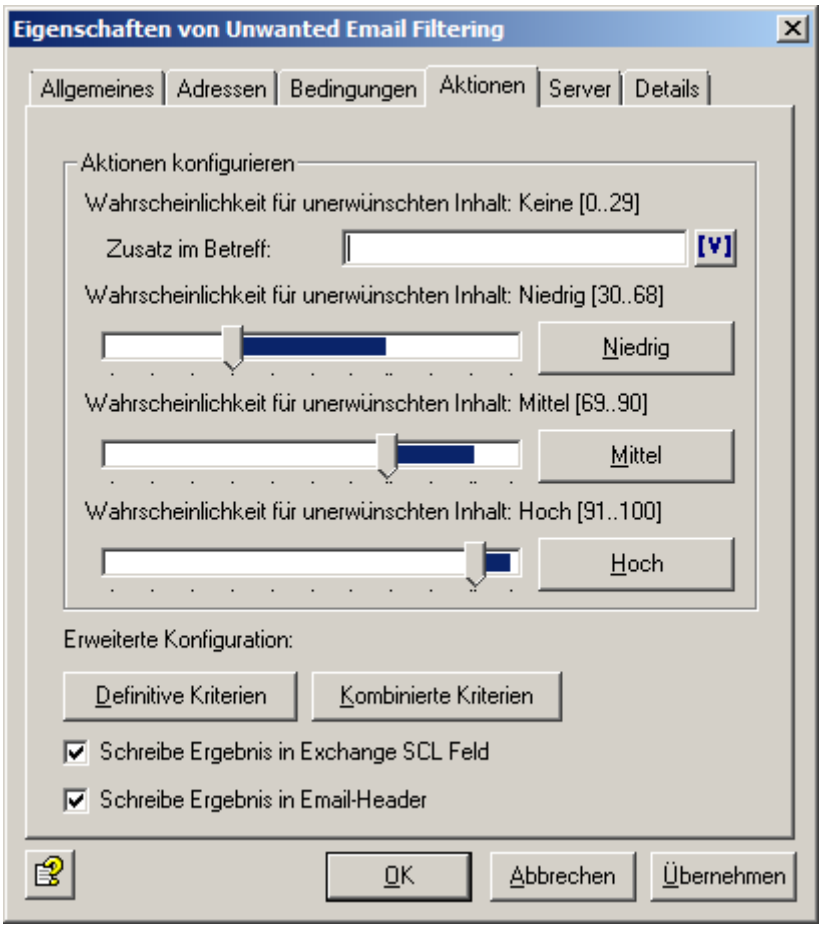
4. Adressbedingungen einrichten.

   Auf der Registerkarte **Adressen** können Sie die Absender und Empfänger eingrenzen, für die dieser Job gültig sein soll. Alle Adressen wählen Sie aus vorhandenen oder selbst erstellten Adresslisten aus.
5. Inhaltliche Bedingungen einrichten.

Auf der Registerkarte **Bedingungen** können Sie die Ausführungsbedingungen eines Jobs festlegen.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

6. Auf der Registerkarte **Aktionen** legen Sie fest, wie hoch die Wahrscheinlichkeit für unerwünschten Inhalt sein soll und was mit gefundenem unerwünschtem Inhalt passieren soll.



Bei hohem Email-Aufkommen können die Quarantänen schnell sehr umfangreich werden und den Email-Durchsatz belasten. Wenn Sie die Emails nicht mehr benötigen, sollten Sie die **Niedrig**- und **Hoch**-Quarantänenkopie deaktivieren.

Es kann für Ihre Produktivumgebung durchaus vertretbar sein, die Wahrscheinlichkeiten für den **Mittel**- und **Hoch**-Bereich anders anzusetzen. Beobachten Sie aber am besten vorher einige Zeit, ob der Job mit dieser Email in Ihrer Produktivumgebung gute Ergebnisse erzielt. Ziel sollte sein:

- Möglichst viel unerwünschter Inhalt in der Quarantäne **Email Filter: Hoch**
- Möglichst viele Ham-Emails in der Quarantäne **Email Filter: Niedrig**
- Möglichst wenige Emails in der Quarantäne **Email-Filter: Mittel**

- **Wahrscheinlichkeit für unerwünschten Inhalt: Keine** (Beispielwerte = 0-30): Normalerweise werden in diesem Bereich keine Aktionen ausgeführt. Klicken Sie die Schaltfläche **[v]**, um einen **Zusatz im Betreff** wie beispielsweise *Avira checked* hinzuzufügen.
- **Wahrscheinlichkeit für unerwünschten Inhalt: Niedrig** (Beispielwerte = 31-69): Klicken Sie die Schaltfläche **Niedrig**, um die Aktionen festzulegen.
- **Wahrscheinlichkeit für unerwünschten Inhalt: Mittel** (Beispielwerte = 70-90): Klicken Sie die Schaltfläche **Mittel**, um die Aktionen festzulegen.
- **Wahrscheinlichkeit für unerwünschten Inhalt: Hoch** (Beispielwerte = 91-100): Klicken Sie die Schaltfläche **Hoch**, um die Aktionen festzulegen.
- Um die definitiven Kriterien für unerwünschten Inhalt anzupassen, klicken Sie **Definitive Kriterien**.
- Um die kombinierten Kriterien für unerwünschten Inhalt anzupassen, klicken Sie **Kombinierte Kriterien**.
- **Schreibe Ergebnis in Exchange SCL Feld**
- **Schreibe Ergebnis in Email-Header**

7. Klicken Sie auf der Registerkarte **Server** die Schaltfläche **Auswählen** und wählen Sie einen Server aus der Liste.

   Damit der Server in der Auswahlliste erscheint, muss er korrekt konfiguriert sein.

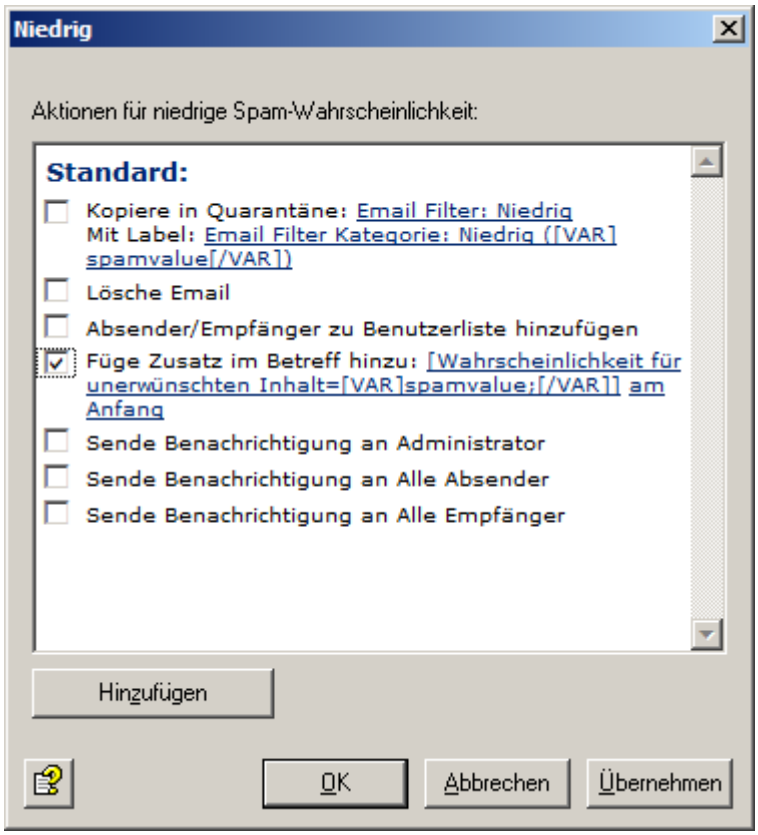
8. Klicken Sie die Schaltfläche **Konfiguration speichern** .

Verwandte Themen:

Emails aus der Quarantäne senden - Seite 24
Geschäftskritische Jobs - Seite 40
Adresslisten - Seite 124
Job-Bedingungen - Seite 151
Einstellungen für einen individuellen Avira Server - Seite 111

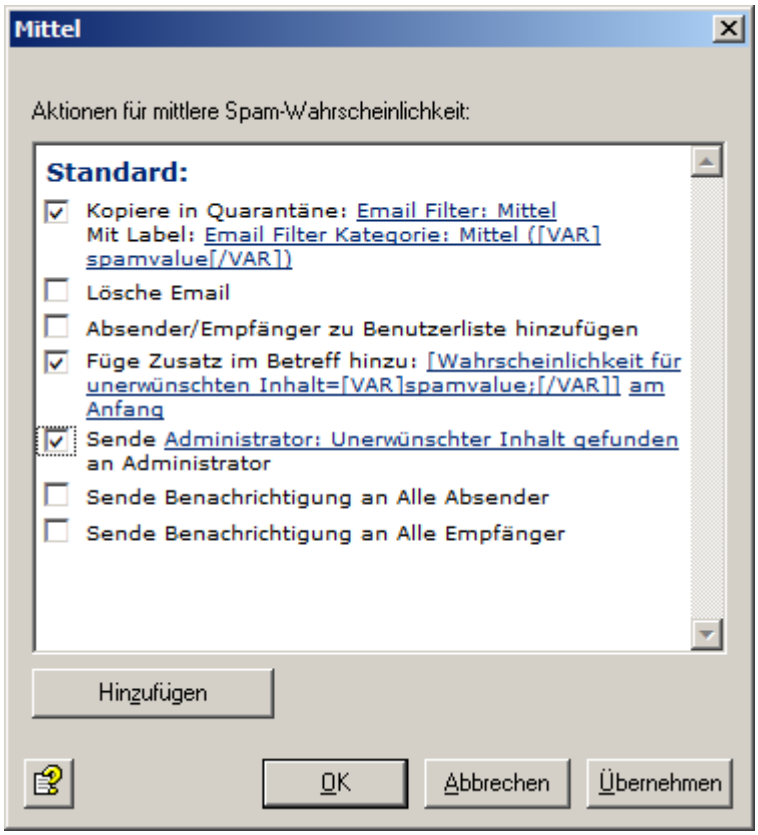
Aktionen bei niedriger Wahrscheinlichkeit für unerwünschten Inhalt

Als einzige Aktion wird die Wahrscheinlichkeit des unerwünschten Inhalts in den Betreff geschrieben. In der Standardkonfiguration ist keine Aktion festgelegt.



Aktionen bei mittlerer Wahrscheinlichkeit für unerwünschten Inhalt

Je höher der Wahrscheinlichkeitswert gesetzt wird, desto eher kann der Empfänger davon ausgehen, dass diese Email nicht oberste Priorität hat. Die mittlere Wahrscheinlichkeit für unerwünschten Inhalt ist für Emails gedacht, bei denen unsicher ist, ob ihr Inhalt erwünscht oder unerwünscht ist. Niedrigere Werte für diese Einstellung bedeuten, dass eine mittlere Wahrscheinlichkeit für unerwünschten Inhalt angenommen werden kann, wenn für einige Kriterien zahlreiche Hinweise oder aber für viele Kriterien eine geringe Anzahl an Hinweisen auf unerwünschten Inhalt gefunden wurden.



Eine Kopie der Email wird in die Quarantäne verschoben und der Administrator wird benachrichtigt. In der Standardkonfiguration wird keine Benachrichtigung an den Administrator gesendet.

Die Original-Email wird dem Empfänger zugestellt. In der Standardkonfiguration wird keine Original-Email zugestellt.

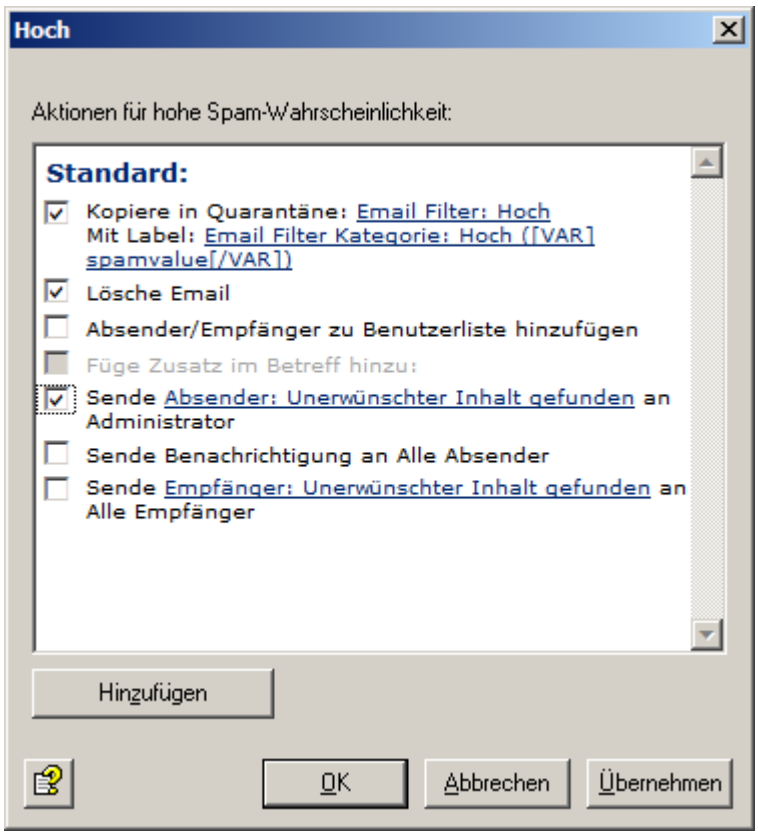
Der Zusatz im Betreff teilt dem Empfänger die Wahrscheinlichkeit für unerwünschten Inhalt in dieser Email mit (beispielsweise *Wahrscheinlichkeit für unerwünschten Inhalt = 75*).

Es ist empfehlenswert, diese Emails in einem eigenen Quarantänebereich (**Email-Filter: Mittel**) zu sammeln und es den Benutzern zu überlassen, was mit diesen Emails geschehen soll.

Die Benutzer können mittels Quarantäne-Sammelbenachrichtigungen über die in einem Quarantänebereich befindlichen Emails mit unerwünschtem Inhalt informiert werden. Sie können die Emails auch mittels des Microsoft-SCL-Wertes durch den Exchange Store direkt in den Junk-Ordner der Benutzer leiten lassen. Durch den konfigurierten Zusatz im Betreff mit der Angabe des Wahrscheinlichkeitswerts für unerwünschten Inhalt kann jeder Benutzer selbst – unter Umständen sogar mit einem Filter in Outlook – die weitere Behandlung dieser Emails festlegen.

Aktionen bei hoher Wahrscheinlichkeit für unerwünschten Inhalt

Die Wahrscheinlichkeit "Hoch" für unerwünschten Inhalt ist für Emails gedacht, die tatsächlich unerwünschten Inhalt enthalten und daher nicht zugestellt werden sollen.



Hier wird die Original-Mail sofort gelöscht und dem Empfänger nicht zugestellt.

Eine Kopie der Email geht in die Quarantäne.

Angesichts des heutigen Aufkommens von Emails mit unerwünschtem Inhalt werden keinerlei Benachrichtigungen an den Administrator versandt.

Ergebnis für unerwünschten Inhalt in Exchange-SCL-Feld schreiben

Ab Service Pack 1 für Exchange 2003 und Outlook 2003 liefert Microsoft einen eigenen Spam-Filter aus. Dieser Intelligent Message Filter (IMF) ermittelt eine Wahrscheinlichkeit dafür, ob es sich bei einer Email um unerwünschten Inhalt handelt.

Das Ergebnis dieser Berechnung ist der so genannte Spam Confidence Level (SCL). Er kann ganze Zahlen zwischen -1 und 9 annehmen. Je höher der SCL, desto größer ist auch die Wahrscheinlichkeit für unerwünschten Inhalt.

Ein SCL von 0 bedeutet, dass höchstwahrscheinlich keine Spam-Mail vorliegt, und -1 wird für Emails vergeben, auf die der Filter überhaupt nicht angewandt wurde, beispielsweise für interne Emails von Absendern aus der gleichen Exchange-Organisation.

Der Exchange-SCL-Wert kann automatisch bestimmte Aktionen auslösen, wie zum Beispiel die Weiterleitung in die Junk-Mail-Ordner der Anwender in Outlook 2003, ohne dass die Anwender selbst aktiv werden müssen.

Im "Exchange System Manager" können Sie zentral definieren, was bei einem bestimmten SCL-Schwellenwert mit den Emails passieren soll. Dabei muss die Aktion nicht auf dem System festgelegt werden, das die Bewertung vornimmt.

Da der IMF den SCL-Wert in die Email schreibt, kann erst das Zielsystem die gewünschte Maßnahme ergreifen. Das Email-Gateway muss hierfür ebenfalls mit Exchange 2003 betrieben werden.

Auch wenn Sie den IMF nicht nutzen können oder möchten, können Sie mit dieser Option den Wahrscheinlichkeitswert für unerwünschten Inhalt des Email-Filtering-Jobs als SCL-Ergebnis festlegen.

Sie können die Exchange-Store-Funktionalität für die möglichen Aktionen bzw. Weiterverarbeitung nutzen. Der Spam-Wahrscheinlichkeitswert wird intern in die SCL-Werte umgerechnet, so dass Outlook sie erkennen kann.

Wenn Sie die Quarantäne-Sammelbenachrichtigungen nutzen, werden die Anwender über alle relevanten Spam-Emails informiert. Sie können in diesem Fall auf die Verwendung der Exchange-Store-Weiterleitung in Junk-Mail-Ordner verzichten. Nähere Informationen über das Exchange-SCL-Feld erhalten Sie unter *http://technet.microsoft.com/en-us/library/bb124426%28v=EXCHG.65%29.aspx*

Email-Filter-Ergebnis in Email-Header schreiben

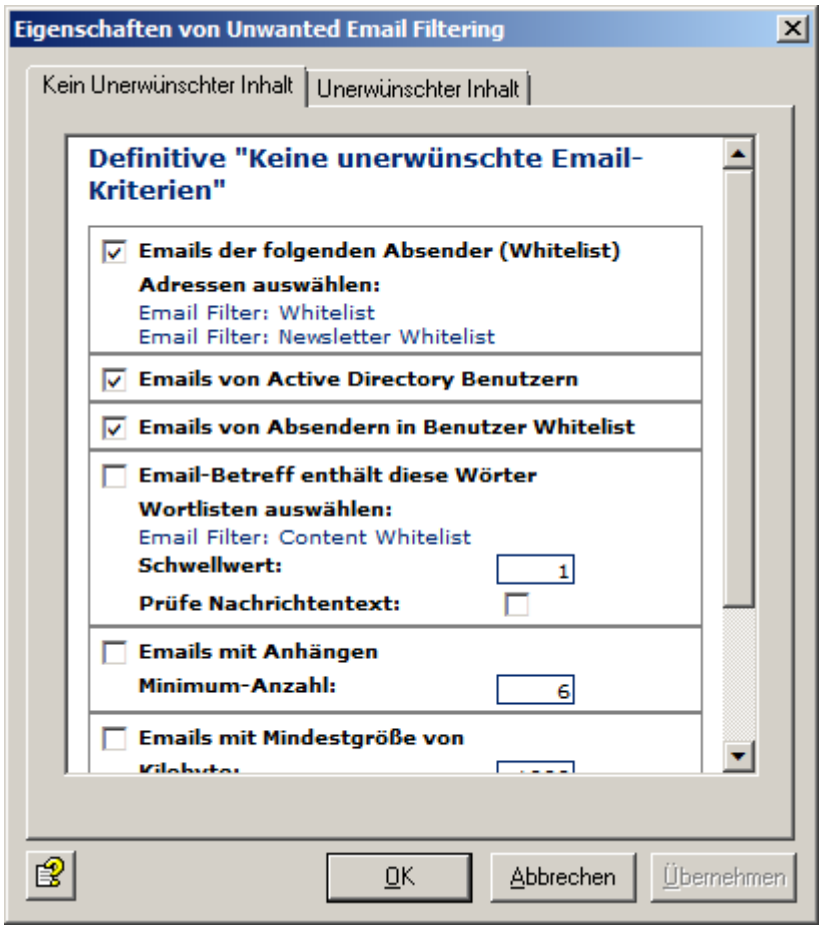
Der Email-Filter-Wert wird für alle drei Wahrscheinlichkeiten (Niedrig, Mittel und Hoch) in den Email-Header geschrieben.

Dazu wird der Ergebniswert in eine Sternenkette umgerechnet (1 Stern bedeutet einen Wert bis zu 10, 2 Sterne bis zu 20, 3 Sterne bis zu 30 usw.), sodass darauf eine Outlook-Regel angewandt werden kann.

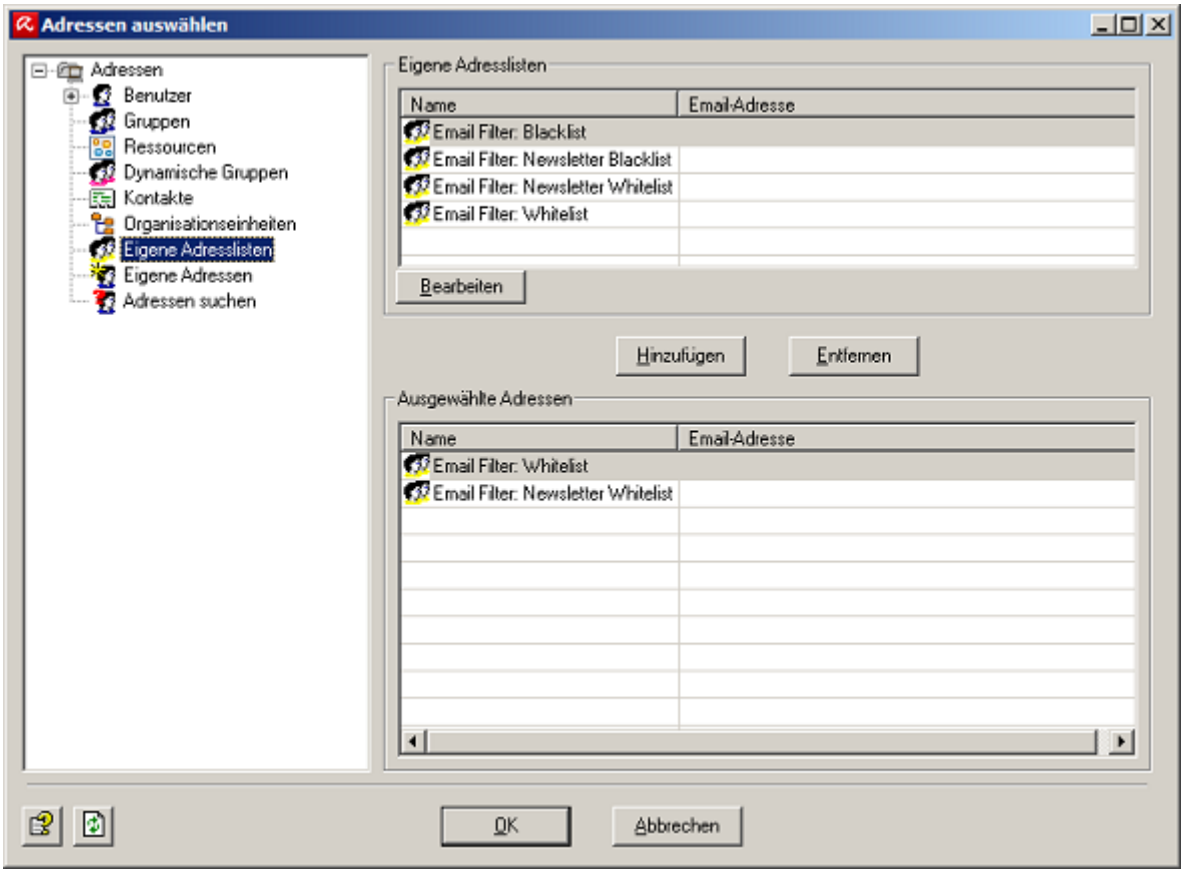
Sie können das Ergebnis auch für jede Email-Filter-Wahrscheinlichkeit einzeln definieren, indem Sie auf der Registerkarte **Aktionen** die Option **Hinzufügen** > **X-Header-Feld hinzufügen** wählen. In diesem Fall wird das Ergebnis nicht in eine Sternenkette umgerechnet, sondern direkt als Wert ausgegeben.

Definitive Kriterien für "Keine unerwünschte Email" festlegen

Whitelists sollten immer aktuell gehalten werden.



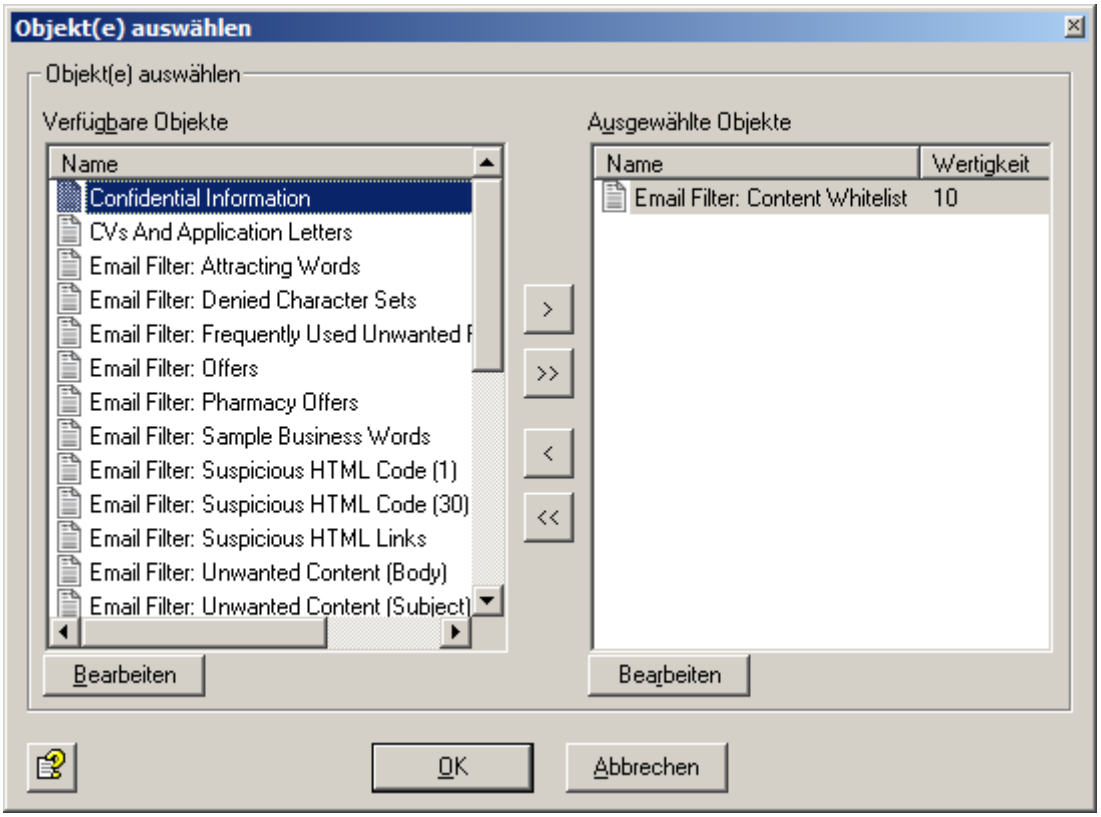
1. Wenn Sie Emails bestimmter Absender immer zulassen möchten, klicken Sie unter dem Kriterium **Emails der folgenden Absender (Whitelist)** auf **Email Filter: Whitelist** und **Email Filter: Newsletter Whitelist**.



2. Wählen Sie hier die Adressen aus oder geben Sie eigene Email-Adressen an, die als Absender immer zugelassen werden sollen, und klicken Sie **OK**.

   Dabei sind die Platzhalter * (Stern) und ? (Fragezeichen) möglich. Sie können also z. B. auch Domänen in der Form `*.domain.com` angeben.

3. Falls Sie die Wortlisten unter dem Kriterium **Email-Betreff enthält diese Wörter** auf der Registerkarte **Kein unerwünschter Inhalt** anpassen möchten, klicken Sie den Link **Email Filter: Content Whitelist**.



- Mit den Pfeiltasten können Sie Wortlisten zur Liste hinzufügen bzw. aus der Liste entfernen.
- Mit den Doppelpfeilen werden alle markierten Wortlisten hinzugefügt bzw. entfernt.
- Klicken Sie die Schaltfläche **Bearbeiten**, um die Eigenschaften einer ausgewählten Wortliste anzupassen.

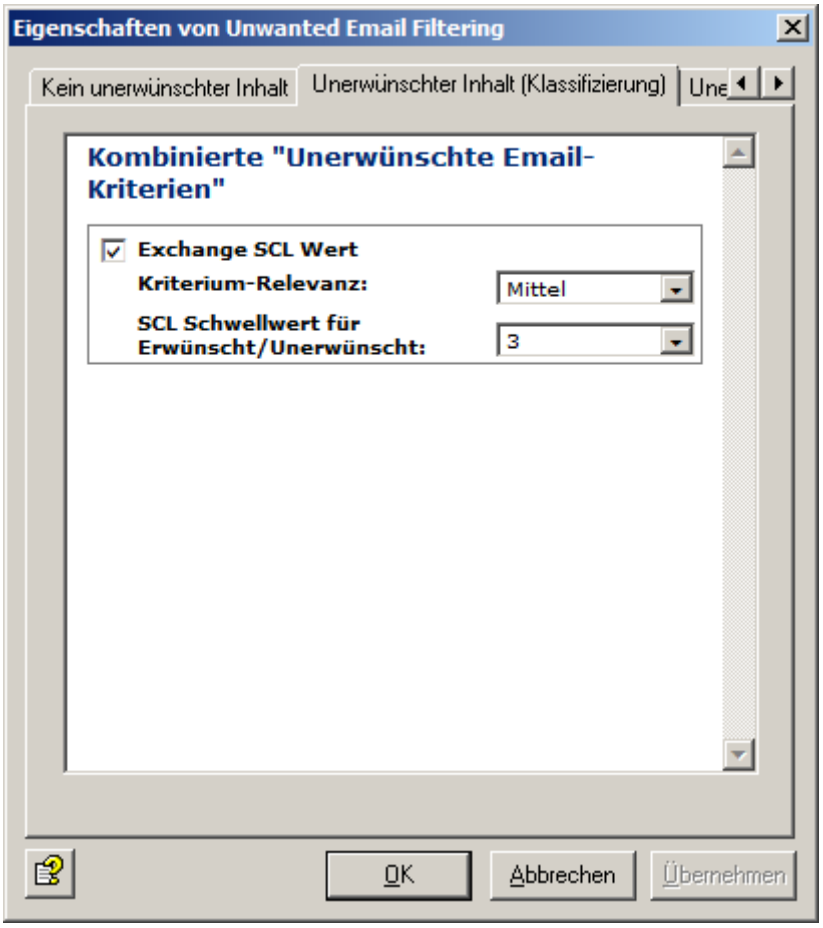
Verwandte Themen:

Definitive Kriterien für erwünschte Emails - Seite 85
Wortlisten erstellen - Seite 74

Kombinierte Kriterien für unerwünschte Emails festlegen

Es wird empfohlen, die Standardeinstellungen des Erweiterte Email-Filterung-Jobs beizubehalten.

1. Wenn Sie die erweiterte Email-Filterung aktivieren möchten, klicken Sie auf der Registerkarte **Aktionen** auf **Kombinierte Kriterien** › **Unerwünschte Email (Klassifizierung)** und aktivieren Sie das Kriterium **Avira Email Filter Ergebnisse**.



2. Legen Sie den Wert für die **Kriterium-Relevanz** fest.

   Der Wert reicht von **Niedrig** bis **Sehr hoch**.

   Die Werte für die Relevanz und den Koeffizienten werden multipliziert und liefern zusammen das Ergebnis für dieses Kriterium.
3. Klicken Sie **OK**.

6.4.4 Email-Filter manuell konfigurieren

Wenn Sie den oben beschriebenen Avira Filterung unerwünschter Emails -Job nicht nutzen möchten, empfiehlt es sich, für eine effektive Email-Filter-Konfiguration folgende Reihenfolge im Jobablauf einzurichten.

Achten Sie auf die richtige Verarbeitungsreihenfolge der Jobs, um die Prüfungen möglichst effektiv und leistungsoptimiert durchzuführen.

1. Legen Sie die Adressprüfung auf bekannte Adressen für unerwünschte Inhalte fest.
2. Legen Sie die Betreffzeilenprüfung auf Text und auf Auffälligkeiten in der Formatierung wie Punkte oder Leerzeichen fest.

   Siehe **Basiskonfiguration** › **Wortlisten** › **Email-Filter: Unerwünschter Inhalt (Betreff)**.
3. Legen Sie die Nachrichtentextprüfung auf Links zu unerwünschten Inhalten (z. B. auch auf Umleitungen und Click-Tracker) fest.

Siehe **Basiskonfiguration** › **Wortlisten** › **Email-Filter: Suspekte HTML-Links**.

4. Legen Sie die Nachrichtentextprüfung auf unerwünschten Text und bekannte typische Auffälligkeiten wie z. B. HTML-Kommentare innerhalb eines HTML-Emailtexts fest.

   Siehe **Basiskonfiguration** › **Wortlisten** › **HTML-Detektor für unerwünschten Inhalt**.

7 Detaillierte Konfiguration

7.1 Basiskonfiguration

In der **Basiskonfiguration** nehmen Sie allgemeine Einstellungen und die wesentlichen Grundeinstellungen für die Module vor.

In der Basis-Konfiguration verwalten Sie:

- Allgemeine Einstellungen wie:

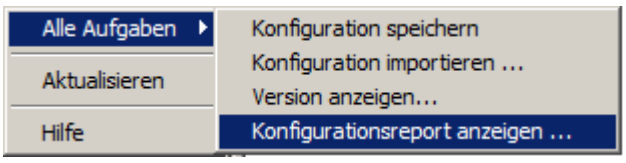
  Proxyserver
  Adresslisten
  Benachrichtigungsvorlagen
  Datenbankverbindungen zu SQL-Servern
  Avira Server
- Ordner (Quarantäne-Ordner)
- Utilities:

  Wortlisten für die Inhaltsprüfung
  Fingerprints für das Blockieren von Anhängen
  Avira Scan Engine
  Avira Email Filter

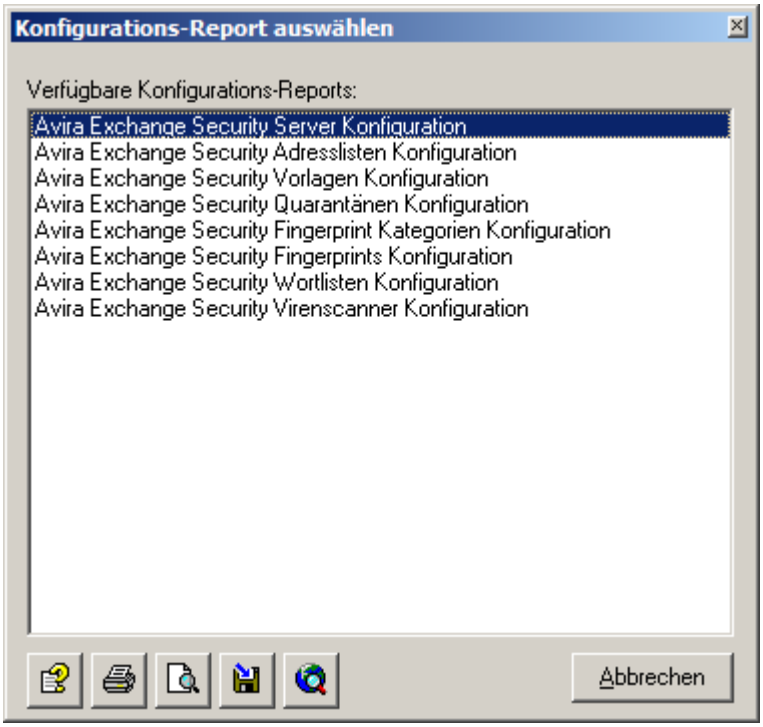
7.1.1 Konfigurationsreports erstellen

Ein Konfigurationsreport gibt einen Überblick über die aktuelle Konfiguration.

1. Klicken Sie mit der rechten Maustaste auf **Basiskonfiguration** und wählen Sie **Alle Aufgaben** > **Konfigurationsreport anzeigen**.



2. Klicken Sie auf den gewünschten Report.


Konfigurations-Report auswählen
Verfügbare Konfigurations-Reports:
Avira Exchange Security Server Konfiguration
Avira Exchange Security Adresslisten Konfiguration
Avira Exchange Security Vorlagen Konfiguration
Avira Exchange Security Quarantänen Konfiguration
Avira Exchange Security Fingerprint Kategorien Konfiguration
Avira Exchange Security Fingerprints Konfiguration
Avira Exchange Security Wortlisten Konfiguration
Avira Exchange Security Virenscanner Konfiguration
Abbrechen

- Klicken Sie auf die Schaltfläche **Konfigurationsreport anzeigen** , um den Report als HTML-Datei im Browser zu öffnen.
- Klicken Sie auf die Schaltfläche **Vorschau Konfigurationsreport** , um sich eine Druckvorschau anzeigen zu lassen.
- Klicken Sie auf die Schaltfläche **Konfigurationsreport speichern** , um den ausgewählten Report als HTML-Datei abzuspeichern.

7.1.2 Konfiguration importieren

Warnung
Bevor Sie eine Änderung eines Objektes der Basis-Konfiguration durchführen, empfiehlt es sich, eine Kopie des alten gleichnamigen Objekts zu erstellen und umzubenennen. Die neue Version ersetzt die alte, so dass anschließend Ihre eigenen Änderungen des Objektes verloren sind.

Warnung
Diese Funktion importiert nicht die vollständige Konfiguration (*ConfigData.xml*) inklusive der Jobs, sondern nur einzelne Basis-Objekte.

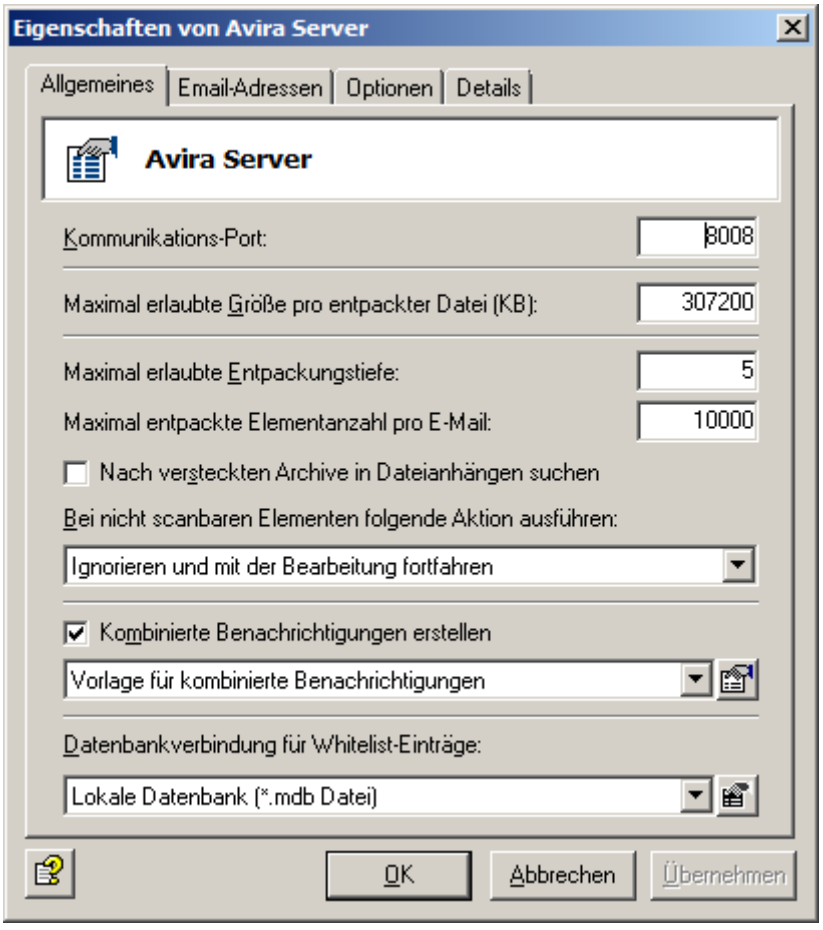
Wenn eine geänderte Version verfügbar ist:

1. Wählen Sie **Basiskonfiguration** › **Alle Aufgaben** › **Konfiguration importieren**, um alle Elemente/Objekte wie z. B. Wortlisten oder Fingerprints neu einzuspielen.
2. Wählen Sie dazu die entsprechende XML-Datei, die Avira zur Verfügung stellt.

7.1.3 Standardeinstellungen für alle Server

Unter **Avira Server Einstellungen**-Einstellungen konfigurieren Sie die Standardeinstellungen für alle Avira Exchange Security-Server. Jeder Server kann zusätzlich individuell konfiguriert werden.

1. Wählen Sie **Basiskonfiguration** > **Allgemeine Einstellungen** aus.
2. Öffnen Sie die Eigenschaften wie folgt:
   - Klicken Sie im rechten Fensterbereich auf **Avira Server Einstellungen** und wählen Sie mit der rechten Maustaste **Eigenschaften**.
   - Doppelklicken Sie **Avira Server Einstellungen**.
   - Klicken Sie im linken Fensterbereich auf **Basiskonfiguration** und wählen Sie mit der rechten Maustaste **Avira Server**.
3. Wechseln Sie zur Registerkarte **Allgemein**.



- **Kommunikationsport**: Für die Kommunikation standardmäßig der Port 8008 verwendet. Diese Angabe gilt für alle Server.

Warnung
Achten Sie auf die korrekte Einstellung Ihres Kommunikationsports für den Avira Monitor. Die Kommunikation mit den Servern ist sonst nicht möglich.

- **Maximal erlaubte Größe...** und **Maximal erlaubte Entpackungstiefe**: Definieren Sie die maximal erlaubte Größe für entpackte Dateien auf der Festplatte und die maximal

erlaubte Entpackungstiefe für Archive. Emails, die diese Werte übersteigen, werden an den **BADMAIL**-Bereich verwiesen.

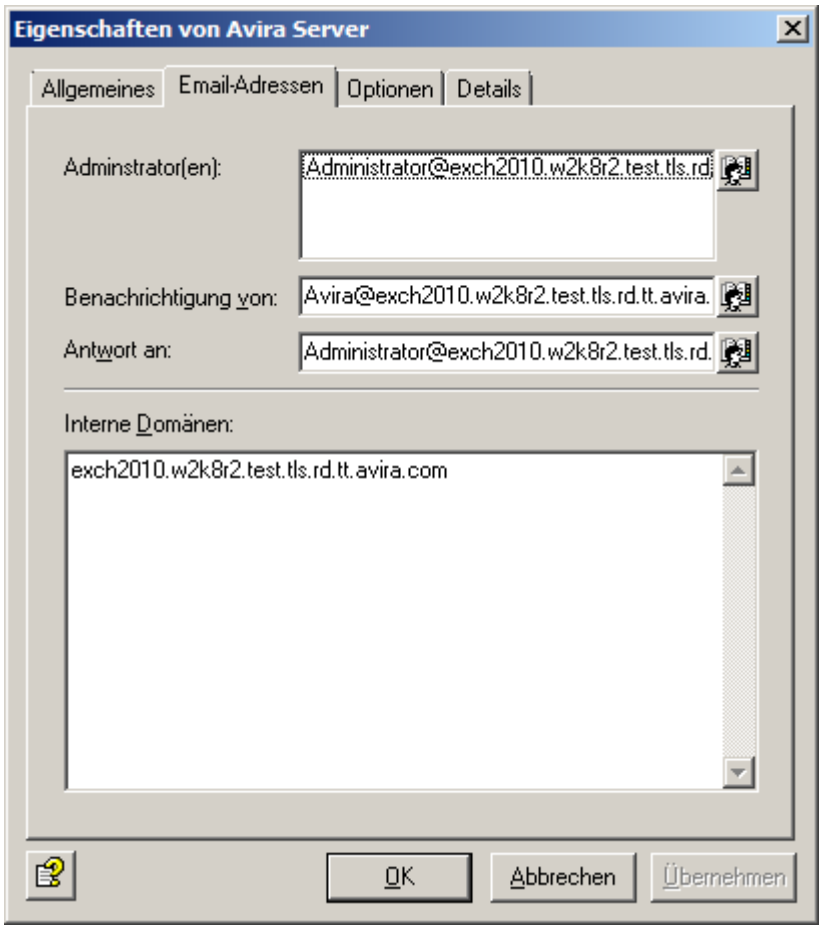
- **Bei nicht scanbaren Elementen**: Für Elemente, die nicht scanbar sind, z. B. Emails mit einem verschlüsselten Anhang, kann eine serverübergreifende Aktion festgelegt werden. Diese wird automatisch ausgeführt, sobald das Programm ein Element als nicht scanbar erkennt. Im Dropdown-Menü stehen zwei Aktionen zur Auswahl. Entweder kann die Tatsache, dass das Element nicht scanbar ist, ignoriert und das Element direkt dem nächsten vorgesehenen Job übergeben werden oder es wird automatisch in die **BADMAIL** Quarantäne verschoben.
- **Kombinierte Benachrichtigungen erstellen**: Die Empfänger dieser Kombinierten Benachrichtigung erhalten also nur eine Email, die alle eingetroffenen Ereignisse gelistet anführt. Als Vorlage wird dazu Kombinierte Benachrichtigungen verwendet. Sie können diese Vorlage modifizieren oder neue Vorlagen anlegen (über **Basiskonfiguration** > **Allgemeine Einstellungen** > **Vorlagen** > **Kombinierte Benachrichtigung**).
- **Datenbankverbindung für Whitelist-Einträge**: Um zentrale Benutzer Whitelists anzulegen, muss zunächst eine Datenbankverbindung zwischen dem SQL-Server und dem Avira Exchange Security-Server konfiguriert werden (**Basiskonfiguration** > **Datenbankverbindung**). Sobald diese Verbindung besteht, wählen Sie in diesem Feld die entsprechende Konfiguration aus.

4. Öffnen Sie die Registerkarte **Email-Adressen**, um Email-Adressen und Interne Domänen zu definieren.

Email-Adressen und interne Domains

Avira Exchange Security benötigt einige Basiseinstellungen zur Maildomäne der zu bearbeitenden Emails. Während der Installation wird die Email-Adresse des angegebenen Avira Exchange Security-Administrators verwendet, um folgende Basiseinstellungen einzutragen:

Diese Einträge gelten für alle Avira Exchange Security-Server. Die Einstellungen können an dieser Stelle jederzeit geändert werden.



- **Administrator(en)**: Die hier eingetragenen Administrator-Adressen erhalten wichtige Status-Benachrichtigungen während der Installation sowie die konfigurierten Administrator-Benachrichtigungen. Als Standardwert trägt die Installation die abgefragte Administrator-Adresse ein.
- **Benachrichtigung von**: Der in den Avira-Benachrichtigungen angezeigte Absender. Als Standardwert trägt die Installation Avira Exchange Security mit der Maildomäne der abgefragten Administrator-Adresse ein.
- **Antwort an**: Der in den Avira Exchange Security-Benachrichtigungen hinterlegte Empfänger von Antworten auf diese Benachrichtigungen. Als Standardwert trägt die Installation die abgefragte Administrator-Adresse ein.
- **Interne Domänen**: Die hier angegebenen Maildomänen werden als interne Maildomänen angesehen, alle übrigen als externe Maildomänen. Diese Einstellung wird verwendet, um im Regelwerk der Avira Exchange Security anhand der Absender- und Empfängeradressen einer Email zu unterscheiden, ob es sich um eine eingehende oder eine ausgehende Email handelt. Ein Email-Filter-Job wird z. B. nur eingehende Emails bearbeiten, während Avira nicht auf ausgehende Emails angewandt werden soll. Mehrere Domänen werden mit **Return** getrennt. Subdomänen werden automatisch eingebunden, wenn vor die Hauptdomäne als Platzhalter das Präfix "*." gestellt wird, beispielsweise `*.domain.com`. Als Standardwert trägt die Installation die Maildomäne der abgefragten Administrator-Adresse ein.

Kombinierte Benachrichtigung

Jeder Job kann generell so konfiguriert werden, dass beim Eintreten eines bestimmten Ereignisses die Empfänger, Absender und/oder die Administratoren über dieses Ereignis benachrichtigt werden (Registerkarte **Aktionen** in **Job-Eigenschaften**).

Treten für eine bearbeitete Email mehrere solche Ereignisse ein, sind die Avira Exchange Security-Emails standardmäßig so eingestellt, dass sie nicht für jedes Ereignis eine separate Benachrichtigung versenden, sondern alle Benachrichtigungen als eine Kombinierte Benachrichtigung verschicken. Die Empfänger dieser Kombinierten Benachrichtigung erhalten also nur eine Email, die alle eingetroffenen Ereignisse gelistet anführt.

Hinweis
Falls Sie den Versand von Kombinierten Benachrichtigungen unterdrücken und stattdessen über jedes eingetretene Ereignis eine Email-Benachrichtigung versenden möchten, deaktivieren Sie unter **Allgemeine Einstellungen** › **Avira Server Einstellungen** › **Allgemein** das Feld **Kombinierte Benachrichtigungen erstellen**.

Zentrale Whitelists einrichten

Findet die Email-Abwicklung in Multi-Server-Umgebungen statt, erzeugt jeder beteiligte Server seine eigenen Benutzer-Whitelists. Ohne Email-Synchronisation erhält folglich jeder Benutzer für jeden der beteiligten Server, eine separate Whitelist, die einzeln gepflegt werden muss.

Um mehrere Whitelists zentral zu verwalten und damit die Administration zu vereinfachen, können Sie anstelle der regulären lokalen Datenbank auf Basis der Microsoft Jet-Engine auch einen Microsoft SQL-Server einrichten, der die Daten für alle beteiligten Avira Exchange Security Server in eine zentrale SQL-Datenbank schreibt.

7.1.4 Erstellen eines Avira Server

1. Klicken Sie unter **Basiskonfiguration Avira Server** und wählen Sie **Neu** › **Avira Server**.
2. Um auf einen neu angelegten Server im **Avira Monitor** sofort zugreifen zu können, aktualisieren Sie die Ansicht (per Rechtsklick auf **Avira Monitor** und **Aktualisieren** auswählen oder über das Symbol in der Symbolleiste).
3. Klicken Sie mit der rechten Maustaste auf den Servernamen, wählen Sie **Eigenschaften** aus und konfigurieren Sie die Einstellungen des neuen Servers.

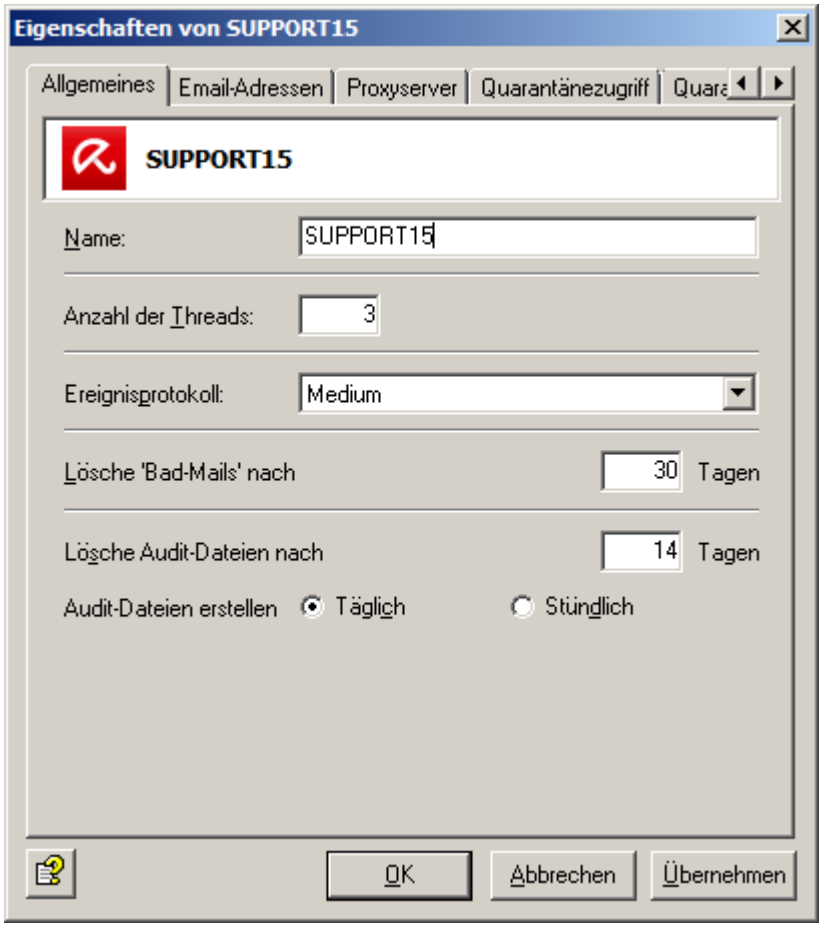
7.1.5 Einstellungen für einen individuellen Avira Server

1. Unter **Basiskonfiguration** klicken Sie **Avira Server** und machen Sie einen Doppelklick auf den Server, den Sie konfigurieren möchten.
2. Nehmen Sie die generellen Einstellungen auf der Registerkarte **Allgemein** vor.
3. Tragen Sie die individuellen Email-Adressen auf der Registerkarte **Email-Adressen**.
4. Legen Sie den Proxyserver auf der Registerkarte **Proxyserver** fest.
5. Bestimmen Sie den Benutzerzugriff auf der Registerkarte **Quarantänezugriff**.
6. Nehmen Sie die Einstellung für die Wartung der Quarantäne auf der Registerkarte **Quarantänewartung** vor.
7. Überprüfen Sie die Liste der auf dem Server angelegten Jobs auf der Registerkarte **AviraJobs**.

Verwandte Themen:

Zugriff auf den Avira Monitor einrichten - Seite 22

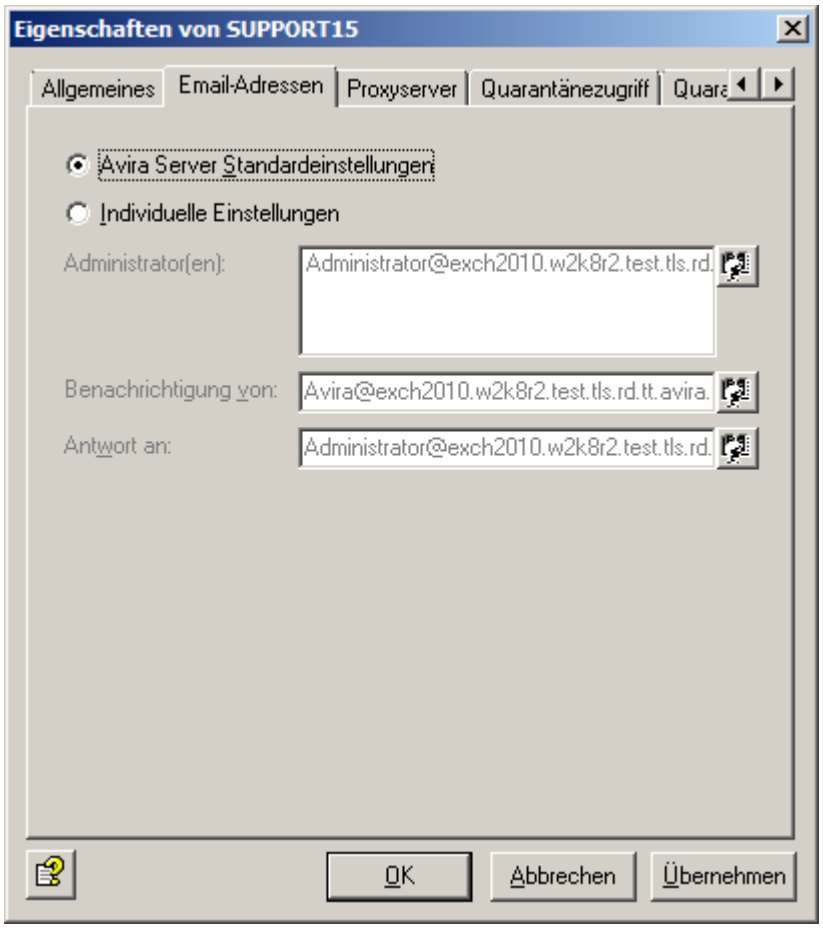
Allgemeine Servereinstellungen



- **Name**: Tragen Sie den Namen des Exchange-Servers ein. Während der Installation wird der aktuelle Exchange-Servername automatisch eingetragen.
- **Anzahl der Threads**: Bestimmen Sie die maximale Anzahl der gleichzeitig bearbeiteten Emails im Feld Anzahl der Threads. Wie viele Emails sinnvollerweise parallel durch Avira bearbeitet werden können, hängt von der Ausstattung und Performance Ihres Servers ab.
- **Protokollstufe für das Ereignisprotokoll**: Wählen Sie die Protokollstufe für das Ereignisprotokoll, welches Sie mit dem Event Viewer/ Ereignisanzeige einsehen können (Windows Event Log). Die Abstufungen reichen von **Kein** bis **Maximum**.
- **Lösche "Bad-Mails" nach**: Bestimmen Sie die Anzahl der Tage, die die Emails in der BADMAIL-Quarantäne verbleiben sollen. Nach Ablauf dieser Tage werden die Emails automatisch gelöscht.
- **Lösche Audit-Dateien nach**: Legen Sie die Anzahl der Tage fest, nach denen ein Audit-Datei im Ordner *Log* gelöscht werden soll.

- **Audit-Dateien erstellen**: Wählen Sie die Frequenz, in der Audit-Dateien erstellt werden sollen (Täglich oder Stündlich).

Individuelle Email-Adressen



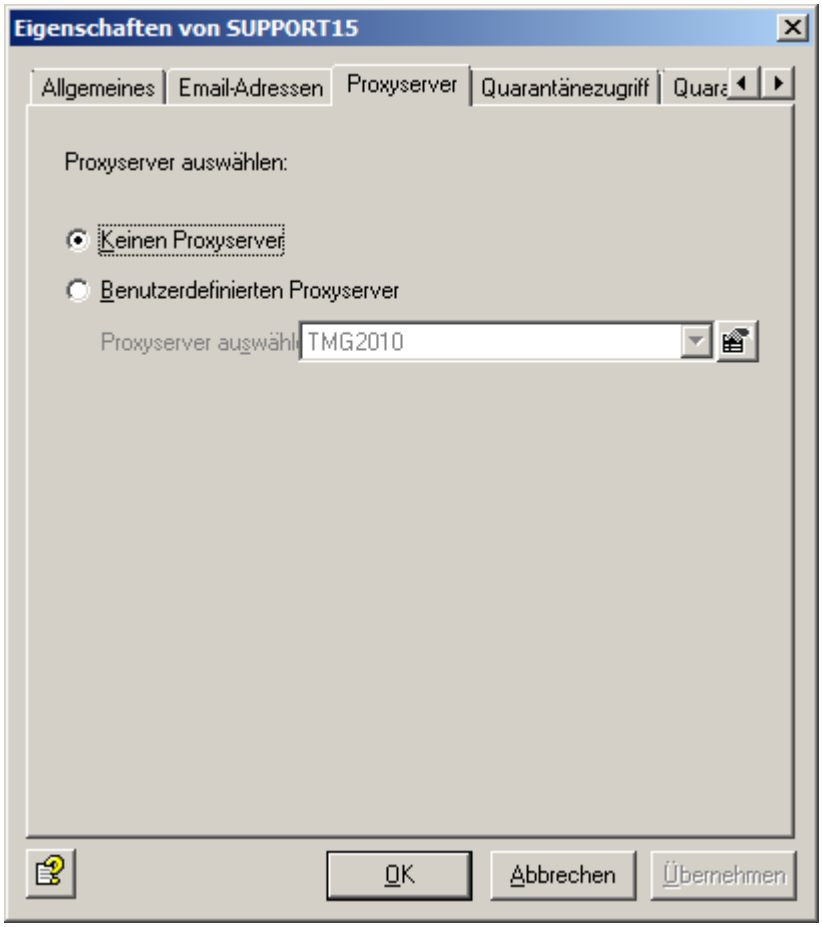
- **Avira Server Standardeinstellungen**: Für jeden einzelnen Server werden die Einstellungen aus den Eigenschaften aller Avira-Servers übernommen, die während der Installation automatisch gesetzt werden oder von Ihnen individuell eingetragen worden sind.
- **Individuelle Einstellungen**: Sollten Sie für einen Server individuelle Einstellungen benötigen, aktivieren Sie diese Option und tragen Sie die Adressen in die entsprechenden Felder ein.

Proxyserver Einstellungen

Wenn in Ihrer Netzwerkumgebung für Internetverbindungen ein Proxyserver erforderlich ist, können Sie für jeden Avira Server Server den passenden Proxyserver auswählen. Beispielsweise für den Download von Updates aus dem Internet.

Hinweis

Wenn Sie die Aktionen des Virusscanner und Avira Email Filter durch einen Proxyserver ausführen lassen möchten, nehmen Sie die entsprechenden Einstellungen auf der Registerkarte **Proxyserver** vor.



Benutzerdefinierter Proxyserver: Wählen Sie einen entsprechenden Proxyserver aus der Liste.

Wenn Sie bereits im Verlauf der Avira Exchange Security-Installation die Verbindungsdaten zum Proxyserver angegeben haben, werden Ihnen diese Proxyserver-Einstellungen unter **Basiskonfiguration** › **Allgemeine Einstellungen** › **Proxyserver** angezeigt

Anderenfalls geben Sie die Proxyserver-Einstellungen dort ein:

- **Name/IP-Adresse**: Vollständiger Name oder IP-Adresse des Proxyservers. Beispiele: `proxy.mydomain.de` oder `127.0.0.1`.
- **Port**: Portnummer des Proxyservers. Der angegebene Port wird für die Kommunikation mit dem Proxyserver verwendet. Beispiel: 8000.
- **Benutzer und Passwort (optional)**: Authentifizierungsdaten, unter dem sich der Updatedienst am Proxyserver anmeldet. Beispiel: `proxy_benutzer`.

Einen Proxyserver löschen Sie, indem Sie mit der Maus einen Rechtsklick ausführen und**Löschen** wählen. Beachten Sie, dass Sie keinen Proxyserver löschen können, der bereits von einem Objekt verwendet wird.

Benutzerspezifischer Zugriff auf die Quarantäne

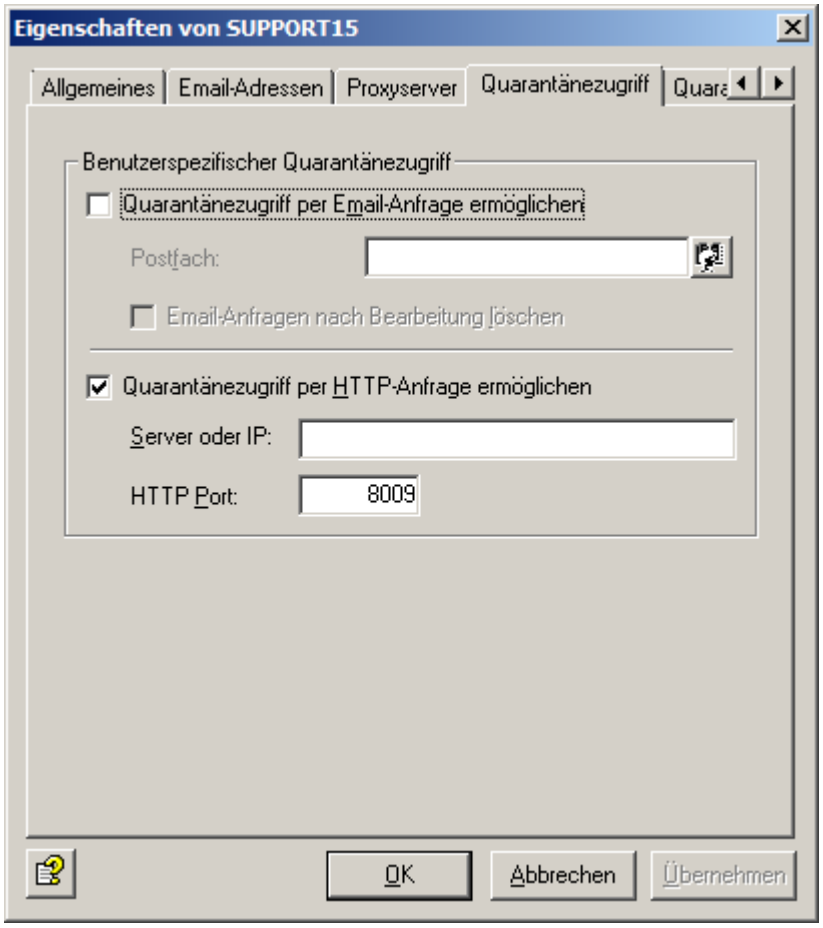
Mit Avira Exchange Security kann der Benutzer selbst auf seine Quarantäne-Emails zugreifen.

Welche Emails das sein sollen und welche Benutzer zugreifen dürfen, kann individuell für jede Quarantäne konfiguriert werden. Diese Funktion ist besonders für Email-Quarantänen bei der Email-Filterung interessant.

Zusätzlich wird der Administrator entlastet, da sich die Benutzer die einzelnen Quarantäne-Emails selbst zustellen können. Sie können für jeden Server definieren, ob und auf welche Art ein Benutzer auf seine Quarantäne-Emails zugreifen darf.

Der Benutzer wird durch eine Quarantäne-Sammelbenachrichtigung über die Quarantäne-Emails informiert, klickt auf die entsprechende Aktion für die gewünschte Email und stellt damit eine Anfrage.

Diese Aktionen werden für jede Quarantäne einzeln konfiguriert und können **Anfordern** (Zustellung an Empfänger der Sammelbenachrichtigung), **Freigeben** (Zustellung an alle Empfänger), **Entfernen** (Email in der Quarantäne zum Löschen vormerken), **Zur Whitelist hinzufügen** oder **Zur Blacklist hinzufügen** sein. Der Zugriff durch den Benutzer erfolgt über eine Email-Anfrage oder über eine HTTP-Anfrage.



- **Quarantänezugriff per Email-Anfrage ermöglichen**: Die Anfrage an die Quarantänen wird über eine Email-Anfrage gestartet.

  Wenn der Benutzer in seiner Quarantäne-Sammelbenachrichtigung auf den Aktionslink für die gewünschte Email klickt, wird die Email-Anfrage automatisch erzeugt und an die Email-Adresse gesendet, die Sie auf dieser Registerkarte im Feld **Postfach** definieren.

  Voraussetzung ist, dass die hier angegebene Email-Adresse existiert und dass die Email über den Server gesendet wird, auf dem Avira Exchange Security und die entsprechenden Quarantänen installiert sind.

  Wir empfehlen, das Postfach auf dem jeweiligen Server anzulegen. Der Inhalt der Email wird ausgelesen und dadurch die vom Anwender gewünschte Aktion durchgeführt. Avira erkennt Anfrage-Emails der Anwender durch:

  - Die Email-Adresse (Angabe im Feld **Postfach**)
  - Das Schlüsselwort für eine Benutzeranfrage in der Email (User Request)

  Letztlich wird die Anfrage-Email im angegebenen Postfach abgelegt.
- **Email-Anfragen nach Bearbeitung löschen**: Die Anfrage-Emails werden nach Abarbeitung aus dem angegebenen Postfach gelöscht.
- **Quarantänezugriff per HTTP-Anfrage ermöglichen**: Die Anfrage an die Quarantäne wird über HTTP gestartet. Der Standardbrowser wird geöffnet, sobald der Benutzer auf die erforderliche Aktion geklickt hat. Der Benutzer erhält eine Meldung, die besagt, dass die Anfrage verarbeitet wird. Für diese Anfrage ist ein freier Port erforderlich. Standardmäßig ist dies Port 8009.

  Die Rückmeldung für den Benutzer, die vom Browser angezeigt wird, ist immer gleichlautend (*OK_Response.html* im Verzeichnis *...\Avira\Avira Exchange Security\AppData*). Sollte die angeforderte Email also nicht mehr existieren, da sie beispielsweise in der Quarantäne bereits gelöscht wurde, erhält der Benutzer keinerlei Benachrichtigung.
- **Eine globale Quarantäne-Sammelbenachrichtigung konfigurieren**: In einer Serverumgebung mit mehreren Avira Exchange Security Servern, die dieselbe Avira Exchange Security Konfiguration mit denselben Quarantänen verwenden, wird empfohlen, eine globale Quarantäne-Sammelbenachrichtigung zu konfigurieren, mit der alle Benachrichtigungen für alle Quarantänen eines Benutzers zu einer Benachrichtigung zusammengefasst werden. Ohne globale Quarantäne-Sammelbenachrichtigungen erhält jeder interne Benutzer von jedem betroffenen Avira Exchange Security Server eine individuelle Sammelbenachrichtigung für jede seiner Quarantänen.

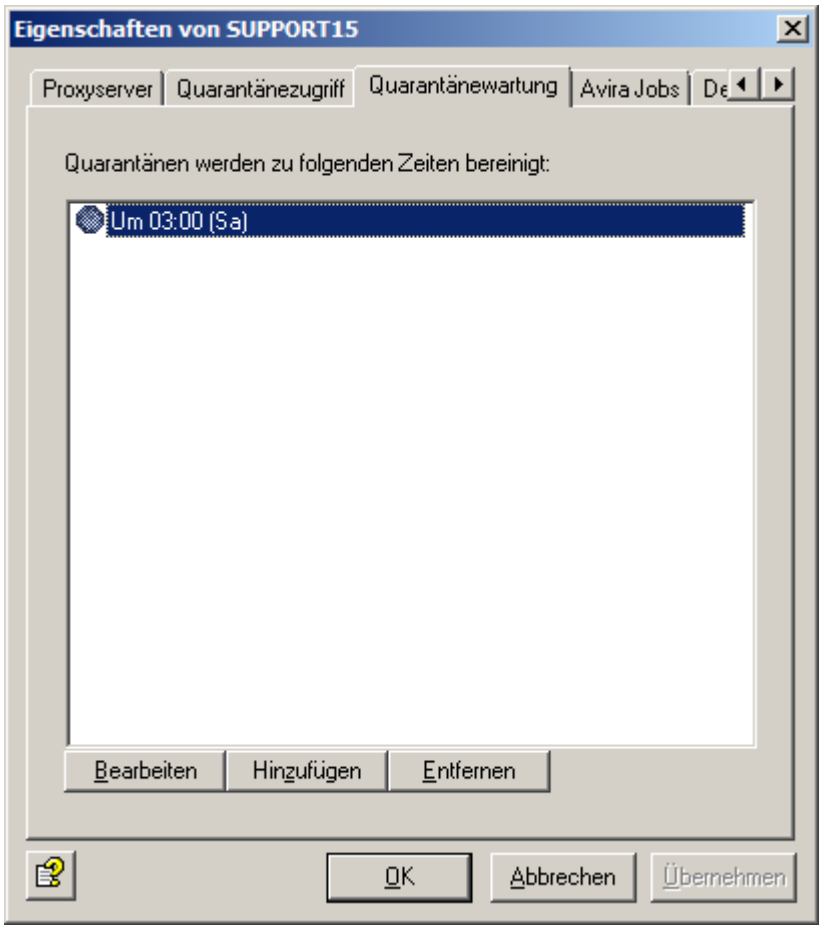
  Geben Sie einen globalen Avira Exchange Security Server an. Auf diesem Server werden alle erforderlichen Quarantänedaten aller betroffenen Quarantänen zu einer globalen Quarantäne-Sammelbenachrichtigung zusammengefasst und an die internen Benutzer gesendet.

1. Öffnen Sie die Avira Server Einstellungen: ALLGEMEINE EINSTELLUNGEN -> Avira Server Einstellungen -> Registerkarte OPTIONEN.
2. Wählen Sie unter **Globaler Avira Server** den Avira Exchange Security Server aus, der als globaler Avira Exchange Security Server definiert werden soll.
3. Geben Sie unter **Benutzer/Passwort** den Namen und das Passwort des Benutzers ein, der über Administratorrechte für alle Quarantänen aller Avira Exchange Security Server verfügt (beispielsweise der Avira Exchange Security Administrator).
4. Definieren Sie, für welche Quarantänen eine globale Quarantäne-Sammelbenachrichtigung erstellt werden soll. Öffnen Sie die gewünschten Quarantänen unter ORDNEREINSTELLUNGEN -> QUARANTÄNE und aktivieren Sie auf der Registerkarte **Sammelbenachrichtigung** die Option zum Erstellen einer globalen Quarantäne-Sammelbenachrichtigung.

Hinweis
Wenn diese Option nicht aktiviert ist, sendet jeder betroffene Avira Exchange Security Server individuelle Sammelbenachrichtigungen für diese Quarantäne.

Quarantänewartung

Legen Sie in dieser Registerkarte den Zeitpunkt fest, zu dem die Quarantänen des Servers bereinigt werden sollen. Durch die Bereinigung werden alle zum Löschen markierten Emails in allen Quarantänen physisch gelöscht und der entsprechende Platz wieder freigegeben.



Die Standardeinstellung für die Bereinigung ist jeden Samstag um 3 Uhr nachts. Falls Sie den Zeitpunkt oder die Häufigkeit ändern möchten, klicken Sie auf **Bearbeiten** und legen Sie die gewünschten Zeiten fest.

Sie können eine Quarantäne bei Bedarf auch manuell bereinigen, indem Sie auf der entsprechenden Quarantäne im **Avira Monitor** mit der rechten Maustaste den Befehl **Alle Aufgaben** › **Quarantäne bereinigen** wählen.

7.2 Datenbankverbindungen

Hinweis
Avira Exchange Security ist für die Verwendung als lokale, eine auf MS Jet Engine basierende, Datenbank optimiert. Im Fall einer komplexen Serverumgebung sind umfassende Konfigurationen für Avira Exchange Security und den MS SQL Server erforderlich, die hier nicht erklärt werden können. Wenn Sie spezifische Fragen haben, wenden Sie sich bitte an unser Support-Team.

Mithilfe der Datenbankverbindungen können Sie externe Datenbanken an Avira Exchange Security anbinden. Anstelle der regulär verwendeten lokalen Datenbank auf Basis der Microsoft Jet-Engine läßt sich so auch ein Microsoft SQL-Server verwenden, der die Avira Exchange Security-Daten in eine SQL-Datenbank schreibt. Zur Zeit können folgende Versionen verwendet werden:

- MS SQL Server 2005
- MS SQL Server 2005 Express, mit eingeschränkter CPU- und Speicherkapazität
- MS SQL Server 2008 R2

Um in Multi-Server-Umgebungen ohne Server-Synchronisation dafür zu sorgen, dass jeder Benutzer nur eine **zentrale Whitelist** für alle beteiligten Server erhält, können Sie einen Microsoft SQL-Server einsetzen. Zusätzlich kann der Microsoft SQL-Server auch mit **Quarantäne-Datenbanken** eingesetzt werden.

Wenn in einer Multi-Server-Umgebung mehrere SQL-Server sowie mehrere Avira Exchange Security Server installiert sind, können diese paarweise angeordnet werden. Das heißt, dass auf jedem Avira Exchange Security Server ein lokaler SQL-Server installiert ist, wodurch nur eine Datenbankverbindung eingerichtet werden muss.

7.2.1 Voraussetzungen für Datenbankverbindungen

Wenn der SQL-Server und der Avira Exchange Security Server auf dem selben Rechner installiert sind, müssen folgende Voraussetzungen gegeben sein:

- Installationen von SQL-Server und Avira Exchange Security Server sind abgeschlossen
- Datenbank(en) sind eingerichtet und die zugehörigen Tabellen angelegt
- Mindestens ein Anwender ist als Datenbankbenutzer angelegt
- Der Datenbankbenutzer hat entsprechende Zugriffsrechte auf die Datenbank
- Der ADO-Treiber ist auf dem Avira Exchange Security Server installiert

Sind der SQL-Server und der Avira Exchange Security Server auf unterschiedlichen Systemen installiert, muss zusätzlich gewährleistet sein, dass:

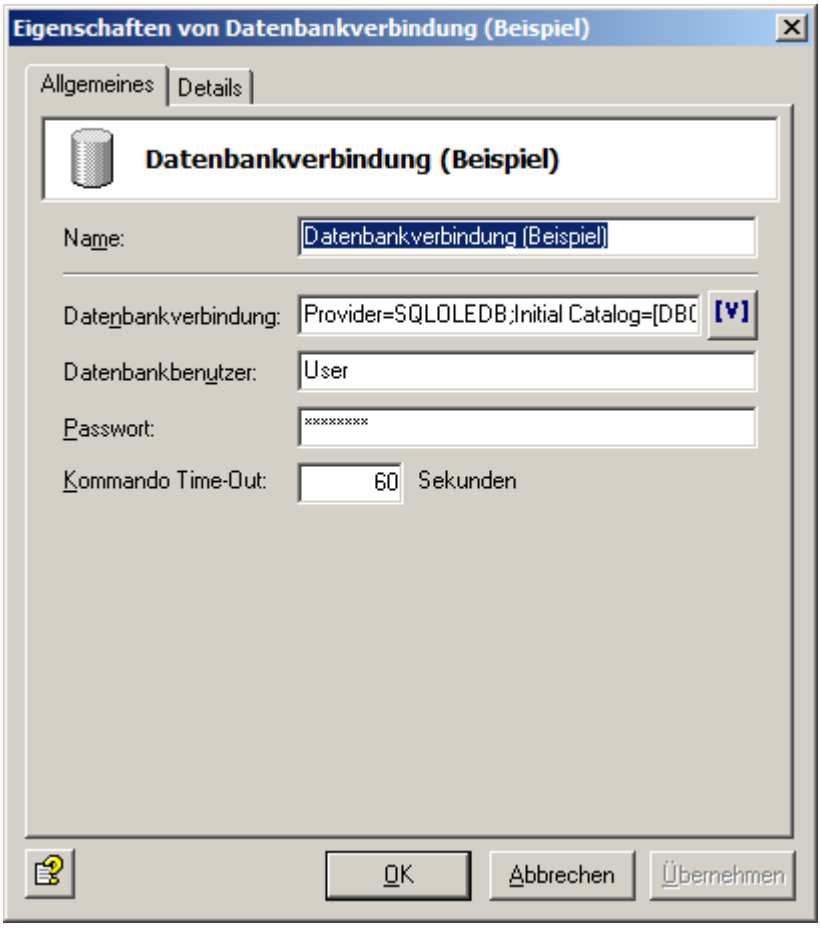
- das auf dem SQL-Server eingestellte Protokoll den Anforderungen zum externen Serverbetrieb entspricht
- nach der Konfiguration des SQL-Servers der Service neu gestartet wurde

7.2.2 Datenbankverbindung konfigurieren

In den folgenden Abschnitten wird die Konfiguration von Datenbankverbindungen zwischen Avira Exchange Security und einem Microsoft SQL-Server beschrieben. Beachten Sie bei der Konfiguration die Unterscheidung zwischen einem zentralen MS SQL Server für zentrale Benutzer Whitelists und einem lokalen MS SQL Server für die Quarantäne.

Die Datenbankverbindung zwischen Avira Exchange Security und dem SQL-Server wird über das ADO-Protokoll hergestellt.

1. Erstellen sie eine neue Datenbankverbindung unter **Basiskonfiguration** > **Allgemeine Einstellungen** > **Datenbankverbindungen**.



2. Vergeben Sie einen Namen für die Verbindungskonfiguration und legen Sie Im Feld **Datenbankverbindung** die Angaben für den ADO-String fest.

   Tragen Sie die benötigten Werte manuell ein oder verwenden Sie die hinterlegten Avira Exchange Security Variablen (Server, Datenbank, usw.), die zur Laufzeit durch die zugehörigen Werte ersetzt werden.

   Ausnahme: Im ADO-String können im Fall eines zentralen SQL-Servers, z.B. bei Verwendung des SQL-Servers für zentrale Whitelists, die beiden Avira Exchange Security Variablen **Server** und **Server (Netzwerk)** nicht verwendet werden. Tragen Sie stattdessen die Bezeichnung des SQL-Servers manuell ein: `Data-Source=Name_des_Servers;`

3. Im Feld **Datenbankbenutzer** tragen Sie den Namen des SQL-Users ein, der auf die Datenbank zugreifen darf (in der Grafik als User eingetragen) und geben Sie im Feld **Passwort** das zugehörige Passwort ein.

   Die hier eingetragenen Werte können über die Variablen `[ADOUser]` und `[ADOPwd]` im ADO-String ausgelesen werden.

4. Im Feld **Kommando Time-Out** geben Sie an, nach wievielen Sekunden die Datenbankverbindung abgebrochen wird, wenn aus der Datenbank keine Daten zurückgeliefert werden.

   Bei großen Datenbanken wird empfohlen mit dem Wert 60 Sekunden zu beginnen.

7.2.3 Beispiel einer ADO-String-Konfiguration

Das nachfolgende Beispiel ist eine von vielen Konfigurationsmöglichkeiten des ADO-Strings. Ausführliche Erklärungen zu diesen und weiteren Optionen und Konfigurationen des MS SQL ADO-Strings, entnehmen Sie bitte der entsprechenden Dokumentation von Microsoft.

Beispiel-Verbindungsstring:

```
Provider=SQLOLEDB;User
 ID=[ADOUser];Password=[ADOPwd];Trusted_Connection=No;Initial
 Catalog=[DBCatalog];Data Source=LOCALHOST\SQLEXPRESS;
```

- `Provider=SQLOLEDB;` Obligatorischer Parameter, der den Provider spezifiziert. Tragen Sie den Wert manuell ein (keine Avira verfügbar).
- `User ID=[ADOUser];Password=[ADOPwd];` Obligatorische Parameter; Schreiben Sie die Parameter `User ID=` und `Password=` manuell in den String und setzen Sie die Avira-Variablen **Datenbankbenutzer** und **Passwort**. Die eingefügten `[ADOUser]` und [ADOPwd] werden bei der Auswertung durch die Inhalte der Felder von Punkt 3 ersetzt. Die Verwendung der Variablen wird empfohlen, da so verhindert wird, dass die Werte im ADO-String in Klartext ausgegeben werden. Prinzipiell können Sie die Werte aber auch manuell eintragen. Lassen Sie in diesem Fall die beiden Felder von Punkt 3 leer.
- `Trusted_Connection=No;` Optionaler Parameter zur SQL-Authentifizierung. Damit der SQL-Server den Avira Exchange Security-Server als Trusted Server kennt, tragen Sie`Trusted_Connection=No;` manuell ein (keine Avira Exchange Security-Variable verfügbar).
- `Initial Catalog=[DBCatalog];` Obligatorischer Parameter, der die zu verwendende Datenbank angibt. Tragen Sie den Parameter `Initial Catalog=’` manuell in den String ein und setzen Sie die Avira Exchange Security-Variable **Datenbank**. Wenn Sie den SQL-Server für die Quarantäne verwenden, wird die Variable `[DBCatalog]` durch den Namen der Datenbank, der unter **Quarantäne** › **Eigenschaften** im Feld **Ordnername** festgelegt wurde, ersetzt. Wenn Sie den SQL-Server dagegen für eine zentrale Whitelist verwenden, wird die Variable `[DBCatalog]` durch den festen Namen `Whitelist` ersetzt. Mittels der Variablen `[DBCatalog]` können Sie eine Datenbankverbindung für mehrere Datenbanken innerhalb eines MS SQL Servers verwenden. Beachten Sie, dass die Datenbanken unter exakt diesem Namen angelegt sein müssen. Ein Verbindungsaufbau ist anderenfalls nicht möglich.
- `Data Source=LOCALHOST\SQLEXPRESS;` Obligatorischer Parameter für einen lokal installierten MS SQL Server 2005 Express. Tragen Sie in diesem Fall den Parameter `Data Source=` manuell ein und setzen Sie bei Bedarf die Avira Exchange Security-Variable Server. Die Variable `[Server]` wird zur Laufzeit durch den NetBiosNamen des Servers ersetzt. Wenn Sie in komplexen Server-Umgebungen mit Subdomains arbeiten, können Sie auch die Avira Exchange Security-Variable **Server (Netzwerk)** verwenden. In diesem Fall wird die Variable `[ServerFQDN]` gesetzt und die FQDN (Fully Qualified Domain Name) des Servers

ausgelesen. Wird der SQL-Server für zentrale Whitelists verwendet, geben Sie hier den Namen des zentralen SQL-Servers manuell an.

7.2.4 Zentrale Whitelists konfigurieren

Findet die Emailabwicklung in Multi-Server-Umgebungen statt, erzeugt jeder Server seine eigenen Benutzer-Whitelists. Ohne Server-Synchronisation erhält folglich jeder Benutzer für jeden der beteiligten Server eine separate Whitelist, die einzeln gepflegt werden muss.

Um diese Whitelists zentral zu verwalten und damit die Administration zu vereinfachen, können Sie anstelle der regulären lokalen Datenbank auf Basis der Microsoft Jet-Engine auch einen Microsoft SQL-Server einrichten, der die Daten für alle beteiligten Avira Exchange Security-Server in eine zentrale SQL-Datenbank schreibt.

Um zentrale Whitelists zu konfigurieren, muss zunächst eine Datenbankverbindung zwischen dem SQL-Server und dem Avira Exchange Security-Server konfiguriert werden. Anschließend sind weitere Einstellungen innerhalb von Avira Exchange Security erforderlich, damit die Einträge aus der Whitelist-Datenbank verwendet werden.

Die Konfiguration der Datenbankverbindung hängt von der Server-Umgebung ab.

1. Geben Sie den zentralen SQL-Server unter `Data Source=` an
   Beachten Sie, dass im ADO-String der Datenbankverbindung die Variable `[DBCatalog]` für die Whitelist-Datenbank durch den festen Datenbanknamen 'Whitelist' ersetzt wird.
2. Wählen Sie unter **Avira Server Einstellungen** › **Eigenschaften** den SQL-Server im Feld **Datenbankverbindung für Whitelist-Einträge** aus.
   In diesem Feld stehen sämtliche Datenquellen, die unter Datenbankverbindungen eingetragen wurden, zur Auswahl.
3. Öffnen Sie den Email-Filter-Job **Erweiterte Email-Filterung**, gehen Sie zu **Aktionen** › **Definitive Kriterien** und aktivieren Sie das Feld **Emails von Absendern in Benutzer Whitelist**.

7.2.5 Quarantäne-Datenbank konfigurieren

Neben der Möglichkeit den Microsoft SQL-Server für Whitelists zu verwenden, kann er auch lokal im Zusammenhang von Quarantäne-Datenbanken eingesetzt werden. Regulär wird der Index einer Quarantäne in der lokalen Datenbank (Microsoft Jet-Engine) geführt. Wenn die Kapazität einer Jet-Datenbank nicht ausreicht, können Sie diese Einträge auch in einen lokal installierten SQL-Server schreiben lassen. Hierfür müssen Sie MS SQL auf dem Email-Server installiert haben.

Die Konfiguration der Datenbankverbindung hängt von der Server-Umgebung ab.

1. Tragen Sie bei Data `Source=` auf jedem Server LOCALHOST ein, um den lokal installierten SQL-Server anzusprechen.
   Beachten Sie, dass im ADO-String der Datenbankverbindung die Variable `[DBCatalog]` für den Namen der Quarantäne-Datenbank, durch den Ordnernamen unter **Quarantäne** ›

Eigenschaften > **Ordnername** ersetzt wird. Dadurch kann eine Datenbankverbindung für mehrere Quarantäne-Datenbanken verwendet werden.

2. Wenn Sie eine Quarantäne als **geschäftskritisch** einstufen möchten, gehen Sie zur **Quarantäne**, klicken Sie mit der rechten Maustaste **Eigenschaften** und aktivieren Sie **Quarantäne ist geschäftskritisch**.

   Bei SQL-Datenbanken ist es mitunter möglich, dass der Datenbank-Service ausfällt oder nicht erreichbar ist. Als Folge ist auch die Quarantäne-Datenbank während dieser Ausfallzeit nicht erreichbar, wodurch Emails, die in diesem Zeitraum in Quarantäne gestellt werden sollten, nicht ordnungsgemäß abgelegt werden können. Um die Behandlung der Email im Quarantäne- Fehlerfall zu steuern, steht ihnen analog zur Option **geschäftskritisch** im Job, die selbe Option auch für die Quarantäne zur Verfügung.

   Ist eine Quarantäne auf **geschäftskritisch** gesetzt, wird ein aufgetretener Quarantänefehler an den Job gemeldet. Daraufhin wird der Job abgebrochen und die Fehlerroutine dieses Jobs gestartet. Wie mit der Email verfahren wird, ob der Job ignoriert oder die Email in das Verzeichnis Badmail verschoben wird, ist abhängig von der Einstellung **geschäftskritisch** im Job selbst.

7.2.6 Handhabung von SQL-Server-Problemen

Treten bei der Installation bzw. Konfiguration der SQL-Server Probleme auf, kann das auf zahlreiche unterschiedliche Ursachen zurückzuführen sein. Daher können an dieser Stelle lediglich Hilfestellungen zur Fehleranalyse gegeben werden:

- Stellen Sie sicher, dass der SQL Server Browser aktiv ist.
- Prüfen Sie den Port (Standard: 1433) oder passen Sie ihn an Ihre Server-Umgebung.
  - Bei **Microsoft SQL Server 2005**: **Configuration Tools** > **SQL Server Configuration Manager** > **SQL Server 2005 Services** > **SQL Server Browser** (Status: *Running*).

Wenn ein zentraler SQL-Server installiert ist, der auf einem anderen Rechner als der Avira-Server läuft, müssen auch folgende Voraussetzungen gegeben sein:

- Wenn Sie den Microsoft SQL Server 2005 verwenden, wählen Sie **Configuration Tools** > **SQL Server Surface Area Configuration** > **Surface Area Configuration for Services and Connections** an. Selektieren Sie bei **MSSQLSERVER** > **Database Engine** > **Remote Connections** die Option **Using both TCP/IP and named paths**, um die im ADO-String konfigurierte Verbindung auf dem SQL-Server zuzulassen.
- Nach der Konfiguration muss der Service des SQL-Servers neu gestartet werden.
- Bei Ausfall des Datenbank-Services beachten Sie auch die Konfigurationsmöglichkeiten der Quarantäne (**geschäftskritisch**).

7.3 Adresslisten

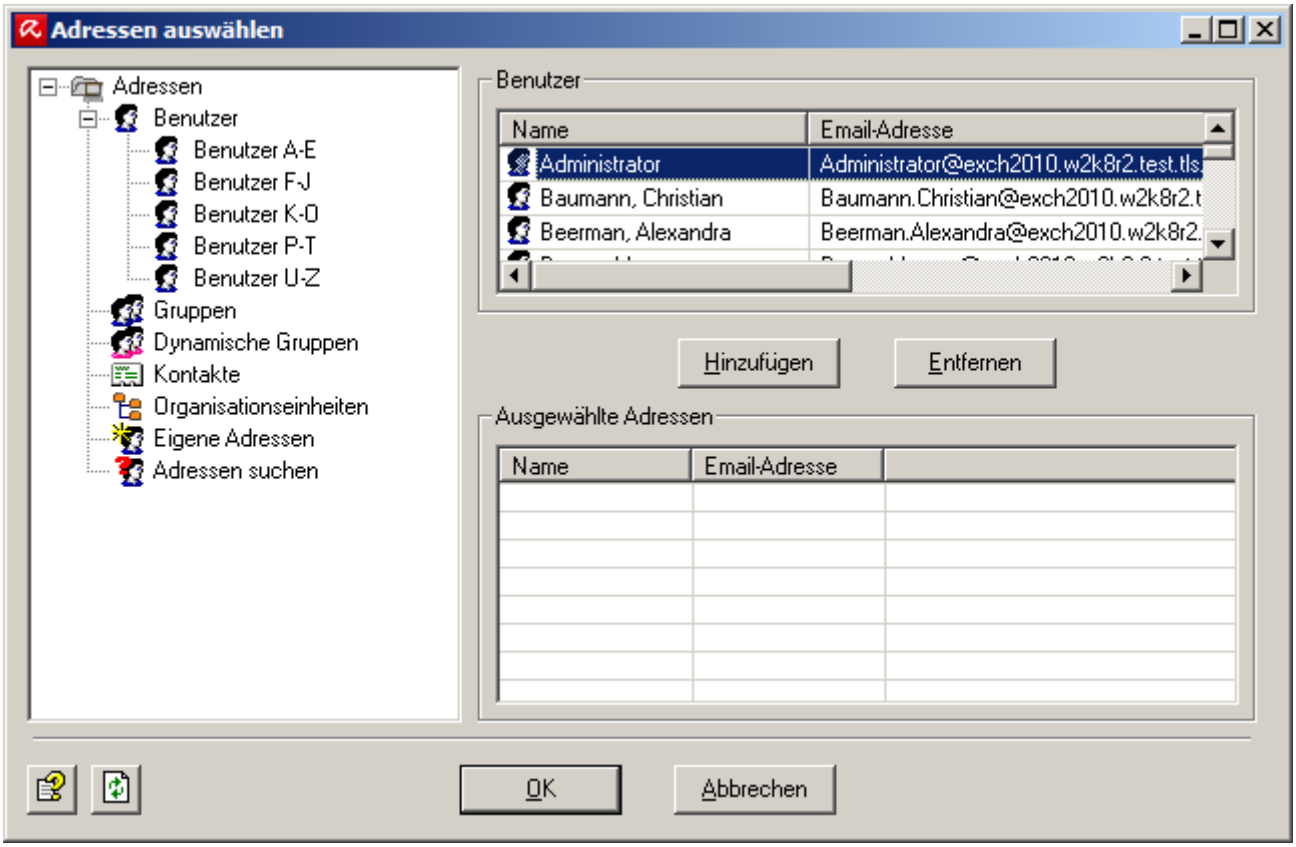
In **Basiskonfiguration** › **Allgemeine Einstellungen** › **Adresslisten** können Sie eigene Adresslisten anlegen, die Sie im Job auswählen. Die zur Verfügung stehenden Adressen werden aus dem Active Directory entnommen.

Verwandte Themen:

Email-Details - Seite 27
Absender einer Adressliste hinzufügen - Seite 26
Emails aus der Quarantäne senden - Seite 24
Avira Monitor - Seite 22
Email-Adressen und interne Domains - Seite 109

7.3.1 Adresslisten erstellen

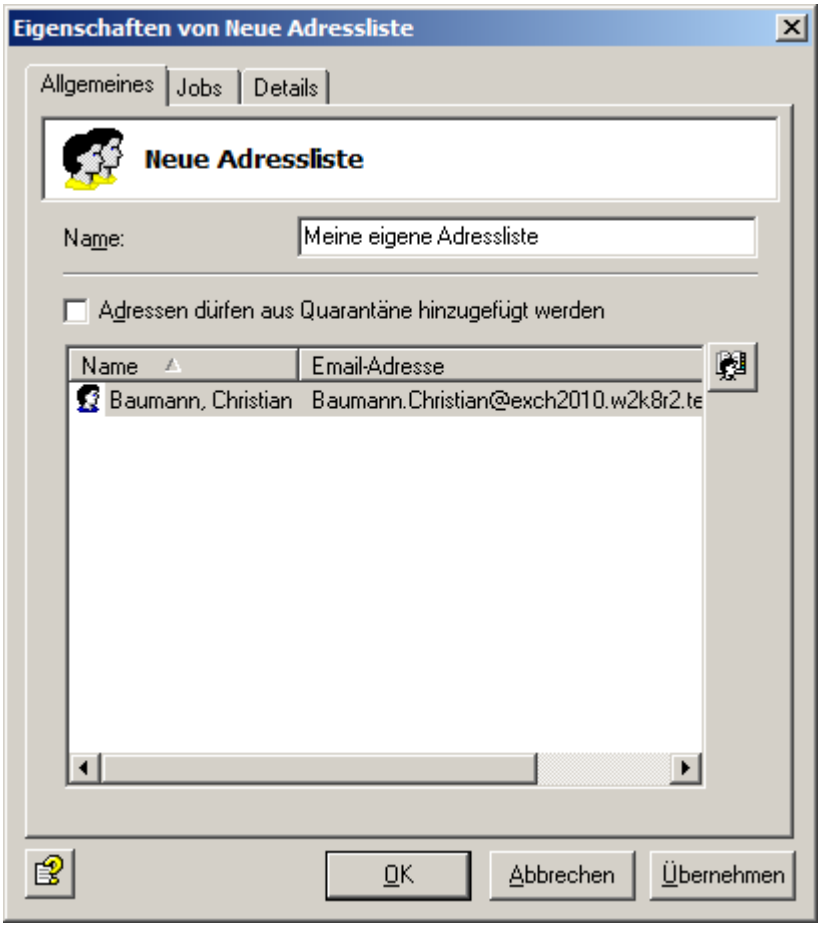
1. Öffnen Sie **Basiskonfiguration** › **Allgemeine Einstellungen**.
2. Klicken Sie mit der rechten Maustaste **Adresslisten** und wählen Sie den Eintrag **Neu** › **Adressliste**.
3. Geben Sie der Adressliste einen Namen.
4. Klicken Sie das Symbol für **Adressen auswählen**: .
5. Im folgenden Fenster wählen Sie aus den einzelnen Rubriken die gewünschten Adressen mit **Hinzufügen** aus.



- Eigene Adressen können Sie in das Eingabefeld eintragen und ebenfalls zur Adressliste hinzufügen. Dabei sind die Platzhalter * (Stern) und ? (Fragezeichen) möglich. Es ist ebenfalls möglich, formal ungültige Email-Adressen wie z. B. `info@domain` einzugeben. Trennen Sie die einzelnen Einträge durch einen Absatz (**Enter**-Taste).
- Sollten Sie eine umfangreiche Liste von eigenen Adressen angelegt haben, so können Sie nach dort enthaltenem Text suchen, indem Sie das Symbol: klicken. Die Textsuche steht Ihnen auch in den Wortlisten zur Verfügung.
- Um einen Eintrag wieder aus der Liste zu löschen, markieren Sie diesen und klicken Sie **Entfernen**.

6. Klicken Sie auf **OK**.

Die Eigenschaften der Adressliste werden geöffnet.



7. Wenn der direkte Zugriff aus einer Quarantäne-Email für diese Adressliste freigegeben sein soll, aktivieren Sie die Option **Adressen dürfen aus Quarantäne hinzugefügt werden**.

Wenn Sie sich im **Avira Monitor** eine Email in einer Quarantäne ansehen, können Sie durch die Schaltfläche **Hinzufügen** die Absenderadresse der Quarantäne-Email zu verschiedenen Adresslisten hinzufügen.

Im Auslieferungsstandard sind folgende Adresslisten für den direkten Zugriff freigegeben:

- Email-Filter: Blacklist
- Email-Filter: Newsletter Blacklist
- Email-Filter: Newsletter Whitelist
- Email-Filter: Whitelist

8. Klicken Sie auf **OK**.

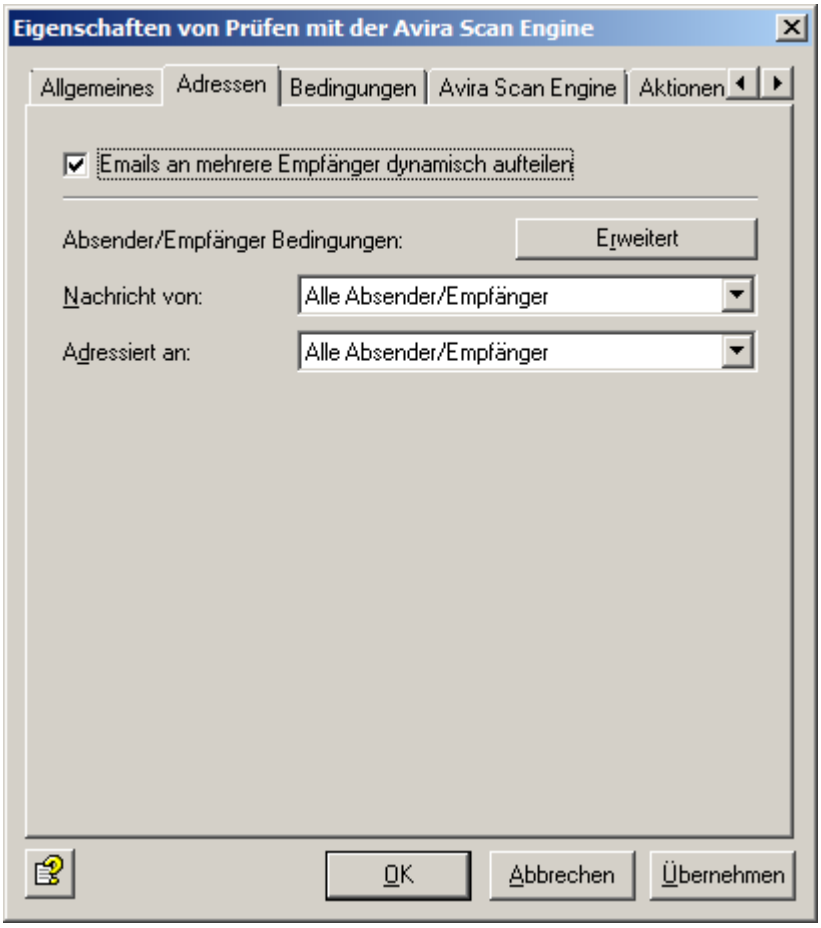
7.3.2 Adressliste löschen

1. Öffnen Sie **Basiskonfiguration** › **Allgemeine Einstellungen**.
2. Klicken Sie mit der rechten Maustaste auf **Adresslisten** und wählen Sie den Eintrag **Löschen** aus dem Kontextmenü.

7.3.3 Adresslisten im Job verwenden

Sie können in jedem Job die Registerkarte **Adressen** verwenden, um auszuwählen von welchen Benutzern der Job angewendet wird.

1. Klicken Sie in den Eigenschaften des Jobs **Adressen**.



- **Emails an mehrere Empfänger bei Bedarf aufspalten (Split)**: Wenn eine Email an mehrere Empfänger adressiert ist, und einer oder mehrere davon in einem Job in der

Adressprüfung eingetragen sind, wird diese eine Email in zwei Emails aufgesplittet: eine Email für die definierten Empfänger der Adressprüfung und eine für die nicht definierten Empfänger. Der Job behandelt dann nur die Email mit den Empfängern, die definiert sind. Es wird nicht gesplittet, wenn Sie keine Adressprüfung für Empfänger definiert haben! Das Splitten der Emails hat Auswirkungen auf die Performance Ihres Servers.

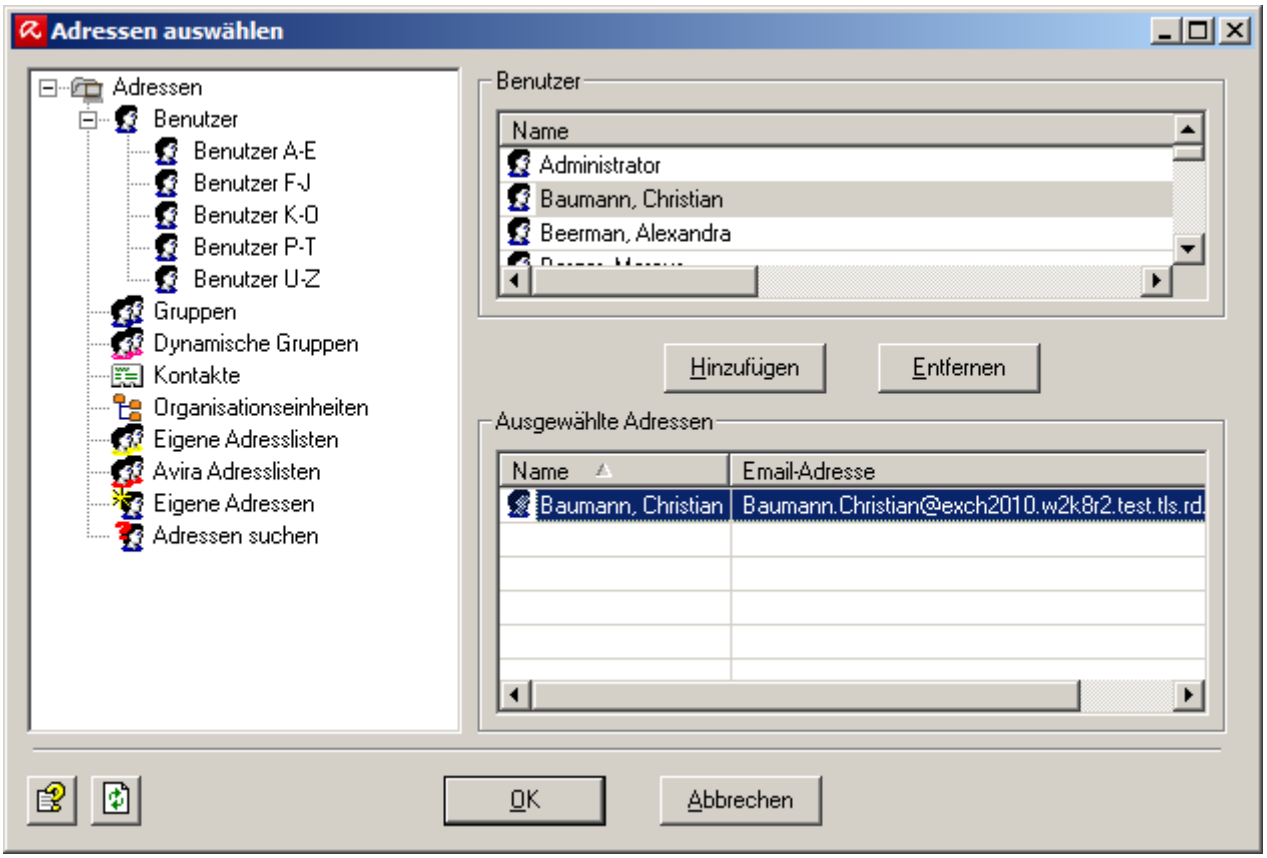
- **Nachricht von** und **Adressiert an**: Wählen Sie, ob der Job für *Alle Absender/Empfänger* zutrifft, oder auf interne oder externe Absender/Empfänger beschränkt sein soll.

Hinweis
Beide Bedingungen in den **Nachricht von** und **Adressiert an** Feldern müssen gegeben sein, damit eine Aktion ausgelöst wird (UND Verknüpfung).

2. Klicken Sie **Erweitert**.

Hinweis
Grundsätzlich müssen alle gegebenen Bedingungen in den Feldern **Aktion wird ausgeführt bei folgenden Absendern** und **Aktion wird ausgeführt bei folgenden Empfängern** zutreffen, damit eine Aktion ausgelöst wird (*UND* Verknüpfung). Wenn mehrere Adressen innerhalb der gleichen Bedingung (z.B. **bei folgenden Absendern**) eingetragen sind, muss nur eine zutreffen, um die Aktion auszulösen. Die Ausnahmen (**gilt aber nicht für ...**) sind für die grundsätzliche Aktionsauslösung irrelevant. Emails für oder von diesen Ausnahmeadressen werden nur weitergereicht, ohne dass die definierten Aktionen ausgeführt werden.

3. Klicken Sie **Interne Absender/Empfänger**, **Keine Adresse ausgewählt** oder einen entsprechenden Eintrag in den Ausnahmen, um das Adressauswahlfenster aufzurufen und die Adressen für genau diese Bedingung zu definieren.



4. Klicken Sie **Avira Adresslisten** im Navigationsbereich, um die definierten Listen für Avira anzusehen.

   Die Avira Adresslisten sind feststehende Listen, aus den Einstellungen der übergreifenden Avira Exchange Security Servers generiert, die bei der Installation abgefragt und eingetragen werden oder die Sie manuell konfiguriert haben.

   Eigene Adresslisten und **Avira Adresslisten** werden nur bei der Adressauswahl für einen Job angezeigt.

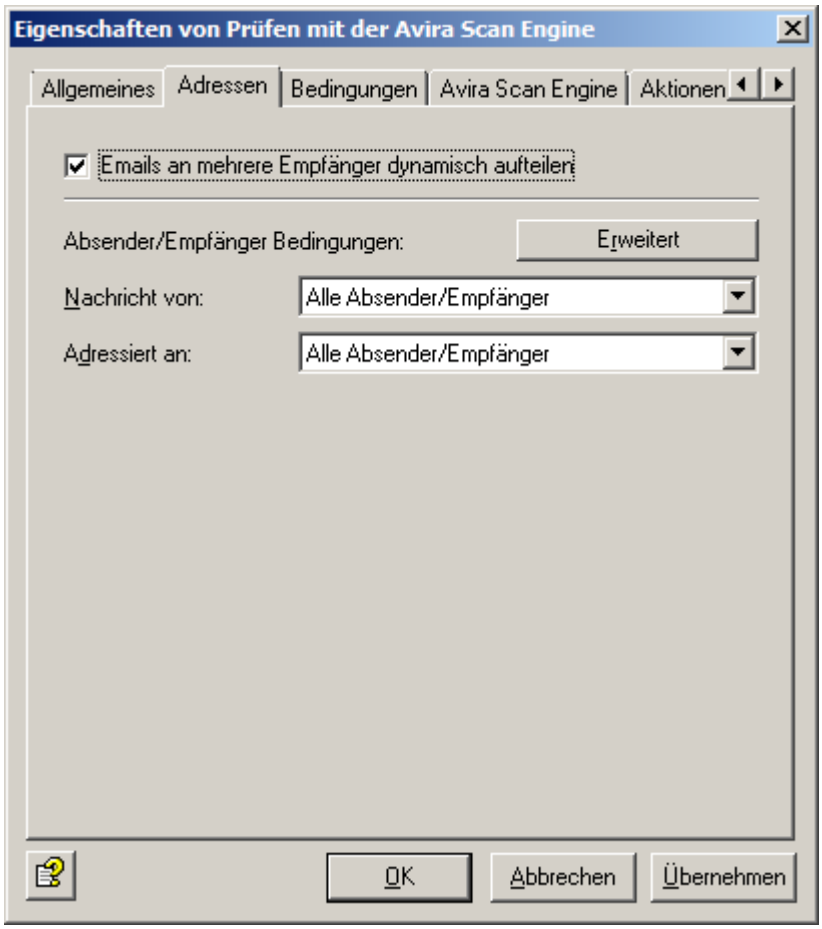
   Eigene Adresslisten können Sie jederzeit ändern, Avira Adresslisten können nicht geändert werden.

7.3.4 Adresseinstellungen wenn auf Viren geprüft wird

Unternehmensrichtlinie: Es sollen alle Emails auf Viren geprüft werden. In diesem Fall kann es nicht genügen, die Emails nur von externen Absendern zu prüfen. Es muss auch sichergestellt werden, dass keine infizierte Email das Unternehmen verlässt. Die definierten Aktionen (Prüfen auf Viren, ggf. Reinigen der Datei und Kopieren in die Quarantäne) müssen also unabhängig von Absender oder Empfänger durchgeführt werden.

Umsetzung: Aktion wird ausgeführt bei **Nachricht von**: *Alle Absender/Empfänger* und bei **Adressiert an**: *Alle Absender/Empfänger*. Es gibt keinerlei Ausnahmen. Jede Email von jedem Absender an jeden Empfänger wird auf Viren geprüft.

Die Darstellung der Adresseinstellungen im Job:



7.3.5 Adresseinstellungen bei blockierten Dateianhängen

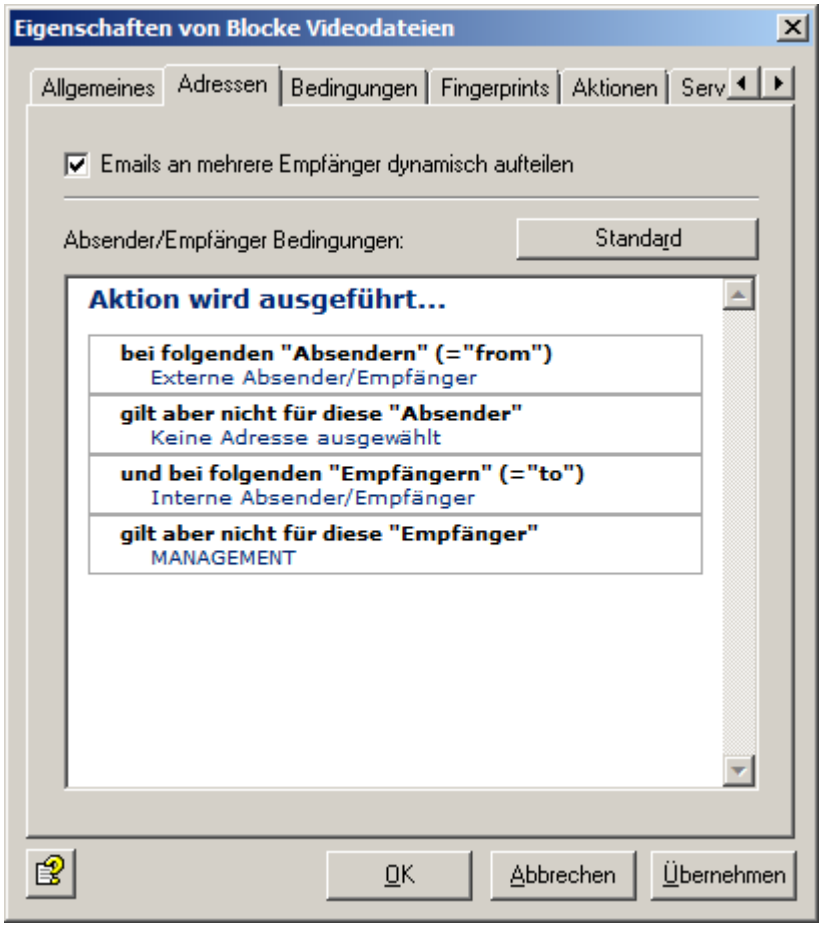
Unternehmensrichtlinie: Es sollen keine Emails über das Internet ins Unternehmen gelangen, die Videoanhänge enthalten. Eine Ausnahme dieser Regel soll aber für das Marketing und die Geschäftsleitung definiert werden.

- **Bei folgenden Absendern** prüft den/die Absender. Die Ausnahme **Gilt aber nicht für diese Absender** ebenfalls.
- **bei folgenden Empfängern** prüft den/die Empfänger. Die Ausnahme **Gilt aber nicht für diese Empfänger** ebenfalls.

Umsetzung: Die definierte Aktion (also das Blockieren der Anhänge) wird unter folgenden Adressbedingungen ausgeführt:

- **bei folgenden Absendern**: *Externe Absender/Empfänger*.
- **bei folgenden Empfängern** an: *Interne Absender/Empfänger*.
- Unter **Gilt aber nicht für diese Empfänger** definieren Sie als Ausnahme die Abteilungen Marketing und Geschäftsleitung, die Sie entweder bereits im Active Directory (AD) als Gruppe eingetragen haben oder die Sie separat als eigene Adressliste anlegen können.

Die Darstellung der Adresseinstellungen im Job:



Damit werden alle Videoanhänge abgefangen, die von externen Absendern an interne Empfänger gesendet werden, es sei denn, der Empfänger ist ein Mitarbeiter des Marketing oder ein Mitglied der Geschäftsleitung.

7.4 Vorlagen

In jedem Job können Sie unter **Aktionen** bestimmen, wer eine Benachrichtigung erhalten soll, wenn Avira Exchange Security eine verbotene Email entdeckt hat.

Beim Anlegen eines neuen Jobs können Sie die entsprechende Vorlage für den Jobtyp auswählen. Die Benachrichtigungsvorlagen für die einzelnen Jobs (Inhaltsprüfung, Virenprüfung usw.) erstellen Sie in der `Basis-Konfiguration`.

7.4.1 Benachrichtigungsvorlagen erstellen

1. Vorkonfigurierte Benachrichtigungsvorlagen für die einzelnen Module finden Sie unter **Basiskonfiguration** › **Allgemeine Einstellungen** › **Vorlagen**.
2. Klicken Sie mit der rechten Maustaste den Vorlagentyp und wählen Sie **Eigenschaften**.
3. Geben Sie einen Betreff für die Benachrichtigung ein.

4. Klicken Sie die Registerkarte **Benachrichtigungstext - Bearbeiten**, um den Text der Benachrichtigung zu bearbeiten.

   Zur Gestaltung des Textes können Sie die Menüleiste für formatierten Text verwenden, die intern in HTMLBefehle umgewandelt werden. Wenn Sie den **Quelltext** mit der Schaltfläche aufrufen, können Sie die HTML-Befehle auch direkt eingeben.
5. Auf der Registerkarte **Jobs** sehen Sie, in welchen Jobs die Benachrichtigungsvorlage verwendet wird.
6. Klicken Sie **OK**.

7.4.2 Liste der Benachrichtigungsvariablen

Folgende Variablen, die Sie auch direkt mit dem Pfeil neben der Schaltfläche **[V]** einfügen können, sind in den Benachrichtigungstexten und in den Betreffzeilen der Benachrichtigungen möglich. Bitte beachten Sie, dass die Tokens `[VAR]` und `[/VAR]` case-sensitiv sind und immer in Großbuchstaben geschrieben werden müssen.

Allgemeine Variablen

Kategorie, Variablentyp	Variable	Beschreibung
Allgemein: Absender	[VAR]Mailsender[/VAR]	Absender der aktionsauslösenden E-Mail
Allgemein: Absender (SMTP)	[VAR]From[/VAR]	Absender-SMTP der aktionsauslösenden E-Mail
Allgemein: Betreff	[VAR]Subject[/VAR]	Betreffzeile der aktionsauslösenden E-Mail
Allgemein: Datum und Uhrzeit	[VAR]Date[/VAR]	Datum und Urzeit, an dem der Job die Aktion auslöste
Allgemein: Datum	[VAR]DateOnly[/VAR]	Datum, an dem der Job die Aktion auslöste
Allgemein: Empfänger	[VAR]Recipients[/VAR]	Empfänger der aktionsauslösenden E-Mail
Allgemein: Job Name	[VAR]Jobname[/VAR]	Name des Jobs, der eine Aktion auslöste
Allgemein: Nicht zutreffende Empfänger	[VAR]UnrestrictedRecipients[/VAR]	Empfänger der aktionsauslösenden Email, die nicht in den Adress (Eingangs)-Bedingungen definiert waren
Allgemein: Quarantäneordner	[VAR]Quarantine[/VAR]	Die Quarantäne, in die eine Email gestellt wurde

Kategorie, Variablentyp	Variable	Beschreibung
Allgemein: Schlüssel einer quarantänierten Email	[VAR]QuarantineDocRef[/VAR]	Allgemein: ID einer Email, die in Quarantäne gestellt wurde
Allgemein: Server	[VAR]Server[/VAR]	Server, über den die betroffene Email gesendet wurde, hier der Name, der in der Konfiguration eingetragen wurde
Allgemein: Server (Netzwerkname)	[VAR]ServerFQDN[/VAR]	Server, über den die betroffene Email gesendet wurde, hier der Netzwerkname des Servers (Fully qualified domain name)
Allgemein: Uhrzeit	[VAR]TimeOnly[/VAR]	Uhrzeit, zu der der aktionsauslösende Job lief
Allgemein: Avira Report	[VAR]ToolReport[/VAR]	Kurze Zusammenfassung der Prüfungsergebnisse
Allgemein: Avira Report (Details)	[VAR]ToolReportDetails[/VAR]	Ergebnis der Prüfungen mit allen Details
Allgemein: Zutreffende Empfänger	[VAR]RestrictedRecipients[/VAR]	Empfänger der aktionsauslösenden Email, die in den Adress (Eingangs)-bedingungen definiert sind

Avira Variablen

Kategorie, Variablentyp	Variable	Beschreibung
Avira: Anhanggröße	[VAR]AttachmentSize[/VAR]	Größe des verbotenen/betroffenen Anhangs
Avira: Anhangtyp	[VAR]FingerprintName[/VAR]	Name des verbotenen Dateityps
Avira: Fingerprintkategorie	[VAR]Fingerprintcategory[/VAR]	Kategorie des verbotenen Dateityps
Avira: Gefundene Email-Größe	[VAR]MessageSize[/VAR]	Größe der gesamten Email
Avira: Gefundener Anhang	[VAR]AttachmentName[/VAR]	Namen der verbotenen/betroffenen Anhänge
Avira: Max. Email-Größe	[VAR]SetSizeLimit[/VAR]	Im Job festgelegte maximale Email-Größe

Kategorie, Variablentyp	Variable	Beschreibung
Avira: Malware Name	[VAR]Virusname[/VAR]	Name der gefundenen Viren
Avira: Suchengine	[VAR]VirusScanner[/VAR]	Namen des Virenscanners

Informationsspeicher-Scan-Variablen

Kategorie, Variablentyp	Variable	Beschreibung
IS-Scan: Datenbank	[VAR]VSAPI_Database[/VAR]	Name des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Datenbank URL	[VAR]VSAPI_Url[/VAR]	URL des Informationsspeichers, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Fehlerbeschreibung	[VAR]VSAPI_ErrorText[/VAR]	Nähere Beschreibung im Fehlerfall durch den Informationsspeicher-Job
IS-Scan: Gesendet am	[VAR]VSAPI_SubmitTime[/VAR]	Sende-Datum und -Uhrzeit der Nachricht
IS-Scan: Nachrichten URL	[VAR]VSAPI_MessageUrl[/VAR]	Informationsspeicher-URL der Nachricht zum Zeitpunkt der Virenprüfung
IS-Scan: Ordner	[VAR]VSAPI_Folder[/VAR]	Name des Informationsspeicher-Ordners, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Postfach	[VAR]VSAPI_Mailbox[/VAR]	Name des Besitzers des Postfaches, in dem sich die Nachricht zum Zeitpunkt der Virenprüfung befunden hat
IS-Scan: Server	[VAR]VSAPI_Server[/VAR]	Name der Servers, auf dem die Virenprüfung durch den Informationsspeicher-Scan durchgeführt wurde

Kategorie, Variablentyp	Variable	Beschreibung
IS-Scan: Suchengine	[VAR]virusscanner[/VAR]	Namen des Virenscanners
IS-Scan: Malware Name	[VAR]virusname[/VAR]	Name der gefundenen Viren
IS-Scan: Zugestellt am	[VAR]VSAPI_DeliveryTime[/VAR]	Zustell-Datum und -Uhrzeit der Nachricht

Avira Email-Filter Variablen

Kategorie, Variablentyp	Variable	Beschreibung
Inhaltsprüfung		
Avira Email-Filter: Details Inhaltsprüfung	[VAR]DeniedContentTabHTML[/VAR]	Detailinformationen über die gefundenen Wörter/Phrasen
Avira Email-Filter: Mailkomponente	[VAR]DeniedMailParts[/VAR]	Betroffene aktionsauslösende Anhänge/Nachrichtentexte
Avira Email-Filter: Verbotene Wortlisten	[VAR]DeniedWordlists[/VAR]	Aktionsauslösende Wortlisten mit erreichtem Wert/Schwellwert
Avira Email-Filter: Verbotene Wörter	[VAR]DeniedWord[/VAR]	Aktionsauslösendes Wort mit erreichtem Wert/Schwellwert
Prüfung auf unerwünschte Email		
Avira Email-Filter: Details der Prüfung auf unerwünschte Email	[VAR]SpamReportHTML[/VAR]	Detailinformationen der einzelnen Kriterien
Avira Email-Filter: Wahrscheinlichkeit für unerwünschte Email	[VAR]SpamValue[/VAR]	Ermittelte Wahrscheinlichkeit für unerwünschte Emails in Form eines Wertes (0 bis 100). Dieser Wert wird mit den individuell einzustellenden Schwellwerten im Erweiterte Email-Filterung-Job verglichen.
Avira Email-Filter: Level für unerwünschte Email	[VAR]SpamLevel[/VAR]	Im Email-Header jeder geprüften Email wird von Avira Email-Filter ein Level für unerwünschte Emails in Form von Sternen in 10er-Schritten eingetragen (XSPAM-TAG:* bedeutet beispielsweise,

Kategorie, Variablentyp	Variable	Beschreibung
		die Wahrscheinlichkeit für unerwünschte Emails liegt zwischen 0 und 10, XSPAMTAG:*** bedeutet hingegen, die Wahrscheinlichkeit für unerwünschte Emails liegt zwischen 20 und 30). Sie können im Header von Outlook nach dieser Zeichenfolge suchen lassen und eine Regel formulieren, die beispielsweise alle Emails mit drei und mehr Sternen mit diversen Aktionen belegt. Nähere Informationen über Regelmöglichkeiten in Outlook entnehmen Sie bitte der Outlook-Hilfe.
Adressprüfung		
Allgemein: Anzahl der Empfänger	[VAR]NumberRecipient[/VAR]	Anzahl der adressierten Empfänger
Avira Email-Filter: Empfänger-Anzahl-Beschränkung	[VAR]SetRecipientLimit[/VAR]	Im Job festgelegte Empfänger-Anzahl-Beschränkung
Avira Email-Filter: Verbotene Absender	[VAR]DeniedSender[/VAR]	Name der aktionsauslösenden Absender
Avira Email-Filter: Verbotene Empfänger	[VAR]DeniedRecipient[/VAR]	Name der aktionsauslösenden Empfänger

Quarantäne-Sammelbenachrichtigungsvariablen

Kategorie, Variablentyp	Variable	Beschreibung
Sammelbenachrichtigung: Absender	[VAR]From[/VAR]	Sammelbenachrichtigung: Absender
Sammelbenachrichtigung: Antwortadresse	[VAR]ReplyTo[/VAR]	Die Adresse, an die Antworten auf die Sammelbenachrichtigung

Kategorie, Variablentyp	Variable	Beschreibung
		geschickt werden sollen (NotificationReplyTo)
Sammelbenachrichtigung: Betreff	[VAR]Subject[/VAR]	Betreff der Sammelbenachrichtigung
Sammelbenachrichtigung: Datum aktuelle Benachrichtigung	[VAR]Nowdate[/VAR]	Datum der Erstellung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Datum letzte Benachrichtigung	[VAR]Lastdate[/VAR]	Datum der Erstellung der letzten Sammelbenachrichtigung
Sammelbenachrichtigung: Datum und Zeit aktuelle Benachrichtigung	[VAR]Now[/VAR]	Datum und Uhrzeit der Erstellung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Datum und Zeit letzte Benachrichtigung	[VAR]Last[/VAR]	Datum und Uhrzeit der Erstellung der letzten Sammelbenachrichtigung
Sammelbenachrichtigung: Empfänger	[VAR]RcptTo[/VAR]	Empfänger der Sammelbenachrichtigung
Sammelbenachrichtigung: Fully Qualified Domain Name (Vollständiger Domainname)	[VAR]FQDN[/VAR]	Vollständiger Netzwerkname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden.
Sammelbenachrichtigung: Liste der Quarantäne Emails	[VAR]HtmlList[/VAR]	Vollständige Liste aller Quarantäne-Objekte für den entsprechenden Empfänger mit HTML-Formatierungen (Pflichtfeld in der Quarantäne-Sammelbenachrichtigung)
Sammelbenachrichtigung: HTTP Port	[VAR]HTTPPort[/VAR]	Port des HTTP-Servers
Sammelbenachrichtigung: HTTP Server	[VAR]HTTPServer[/VAR]	HTTP-Server, um eine Benutzeranfrage per HTTP zu versenden

Kategorie, Variablentyp	Variable	Beschreibung
Sammelbenachrichtigung: Quarantäne	[VAR]Displayname[/VAR]	Name der Quarantäne, aus der die Liste der Emails erstellt wurde
Sammelbenachrichtigung: Server	[VAR]Server[/VAR]	Kurzname des Servers, auf dem sich die Quarantäne befindet, für die die Sammelbenachrichtigungen erzeugt werden
Sammelbenachrichtigung: Uhrzeit aktuelle Sammelbenachrichtigung	[VAR]Nowtime[/VAR]	Uhrzeit der Generierung der aktuellen Sammelbenachrichtigung
Sammelbenachrichtigung: Uhrzeit letzte Sammelbenachrichtigung	[VAR]Lasttime[/VAR]	Uhrzeit der Erstellung der letzten Sammelbenachrichtigung

Variablen für kombinierte Benachrichtigungen

Kategorie, Variablentyp	Variable	Beschreibung
Kombinierte Benachrichtigung: Inhaltsverzeichnis	[VAR]TOCList[/VAR]	Nummerierte HTML-Liste aller Benachrichtigungen (Subject). Jeder Listeneintrag ist per Link mit dem zugehörigen Eintrag der Benachrichtigungsliste (Variable "NotificationList") verknüpft.
Kombinierte Benachrichtigung: Benachrichtigungsliste	[VAR]NotificationList[/VAR]	HTML-Liste aller Benachrichtigungen (Body) jeweils durch einen waagerechten Trennstrich abgegrenzt.

Whitelist Variablen

Kategorie, Variablentyp	Variable	Beschreibung
Userlist: Einträge	[VAR]HtmlList[/VAR]	Komplette Liste aller Einträge für den entsprechenden Empfänger mit HTML-Formatierungen

Kategorie, Variablentyp	Variable	Beschreibung
		(Pflichtfeld in der Whitelist-Benachrichtigung).
Userlist: Fully qualified domain name	[VAR]FQDN[/VAR]	Voller Netzwerkname des Servers, auf dem sich die Whitelist befindet, für die die Sammelbenachrichtigungen erzeugt werden.
Userlist: HTTP-Port	[VAR]HTTPPort[/VAR]	Port des HTTP-Servers
Userlist: HTTP-Server	[VAR]HTTPServer[/VAR]	HTTP-Server, um eine Benutzeranfrage per HTTP zu versenden
Userlist: Namen anzeigen	[VAR]Displayname[/VAR]	Name der Whitelist, aus der die Liste der Emails erstellt wurde
Userlist: Empfänger	[VAR]RcptTo[/VAR]	Empfänger der Whitelist-Benachrichtigung
Userlist: Antwortadresse	[VAR]ReplyTo[/VAR]	Die Adresse, an die Antworten auf die Whitelist Benachrichtigung geschickt werden sollen (NotificationReplyTo)
Userlist: Absender	[VAR]From[/VAR]	Absender der Whitelist-Benachrichtigung
Userlist: Server	[VAR]Server[/VAR]	Kurzname des Servers, auf dem sich die Whitelist befindet, für die die Benachrichtigungen erzeugt werden
Userlist: Größe	[VAR]CollectedSize[/VAR]	Gesamtgröße der Whitelist Benachrichtigung
Userlist: Betreff	[VAR]Subject[/VAR]	Betreff der Benachrichtigung
Userlist: Nummer der Benachrichtigung	[VAR]SummaryPart[/VAR]	Wenn mehr als 3.000 neue Einträge in einer Whitelist aufgeführt werden, erhält der Anwender mehrere Whitelist-Benachrichtigungen. Die Variable gibt die fortlaufende

Kategorie, Variablentyp	Variable	Beschreibung
		Nummer der Benachrichtigung zurück ("1" für die ersten 3.000 Einträge, "2" für die nächsten 3.000 Einträge usw.).
Whitelist: Whitelist per HTTP versenden	[VAR]link::HTTP_SendWhitelist[/VAR]	Whitelist-Anfrage und Benachrichtigung erfolgt über HTTP
Whitelist: Whitelist per Email versenden	[VAR]link::MAIL_SendWhitelist[/VAR]	Whitelist-Anfrage und Benachrichtigung erfolgt per Email
Whitelist: Whitelist per HTTP löschen	[VAR]link::HTTP_ClearWhitelist[/VAR]	Löschen der Whitelist über HTTP
Whitelist: Whitelist per Email löschen	[VAR]link::MAIL_ClearWhitelist[/VAR]	Löschen der Whitelist per Email
Blacklist: Blacklist per HTTP versenden	[VAR]link::HTTP_SendBlacklist[/VAR]	Blacklist-Anfrage und Benachrichtigung erfolgt über HTTP
Blacklist: Blacklist per Email versenden	[VAR]link::MAIL_SendBlacklist[/VAR]	Blacklist-Anfrage und Benachrichtigung erfolgt per Email
Blacklist: Blacklist per HTTP löschen	[VAR]link::HTTP_ClearBlacklist[/VAR]	Löschen der Blacklist über HTTP
Blacklist: Blacklist per Email löschen	[VAR]link::MAIL_ClearBlacklist[/VAR]	Löschen der Blacklist per Email

7.5 Konfiguration der Quarantäne

Eine Quarantäne ist ein Ordner, in dem alle von den Bedingungen betroffenen Emails gespeichert werden, wenn Sie dies mithilfe der Aktion **In Quarantäne kopieren** so festgelegt haben.

Bei der Installation von Avira Exchange Security, wird ein Ordner namens *Quarantäne* im Dateiverzeichnis (...*Avira**Avira Exchange Security**AviraData*). Dieser Ordner enthält anfänglich einige Standard-Quarantänen und später alle zusätzlichen neu erstellten Quarantänen.

Verwandte Themen:

Zugriff auf den Avira Monitor einrichten - Seite 22

7.5.1 Eine neue Quarantäne erstellen

Warnung
Die Größe einer Quarantäne ist auf 1 GB beschränkt.

1. Gehen Sie zu **Basiskonfiguration** > **Ordner** > **Quarantäne**.
   Alle verfügbaren Quarantänen werden im rechten Fenster angezeigt.
2. Klicken Sie mit der rechten Maustaste **Quarantäne** und wählen Sie **Neu** > **Quarantäne**.

   Der **Ordnername** aus der Beschreibung wird übernommen. Dabei werden nur die Zeichen von A-Z und von 0-9 umgesetzt, alle anderen Zeichen werden in Unterstriche umgewandelt.
3. Wenn Sie den in **Ordnername** vorgeschlagenen Namen ändern möchten, geben Sie einen Quarantänenamen ein.

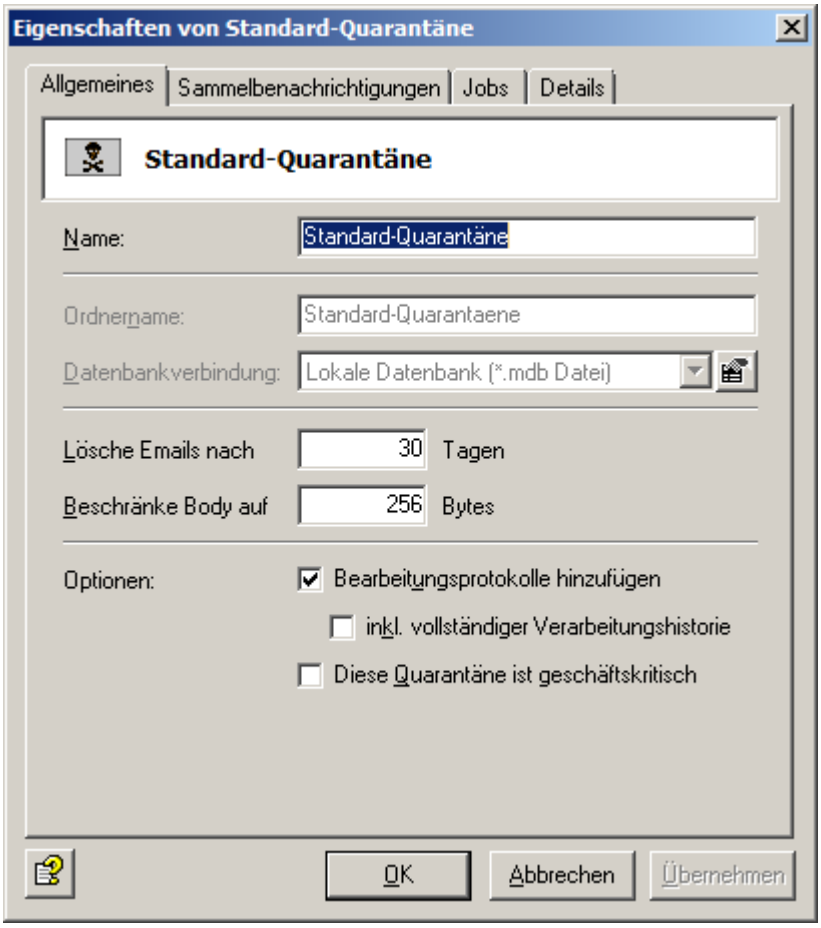
   Geben Sie keinen absoluten Pfad ein, sondern nur den Ordnernamen.
4. Speichern Sie die Konfiguration.

   Die neue Quarantäne wird automatisch vom EMH angelegt. Anschließend wird sie auch im Avira Monitor angezeigt, wenn Sie die Ansicht aktualisieren.

7.5.2 Quarantäne konfigurieren

Warnung
Die Größe einer Quarantäne ist auf 1 GB beschränkt.

1. Gehen Sie zu **Basiskonfiguration** > **Ordner** > **Quarantäne**.
   Alle verfügbaren Quarantänen werden im rechten Fenster angezeigt.
2. Klicken Sie mit der rechten Maustaste eine Quarantäne in der Liste und wählen Sie **Eigenschaften**.



- **Name**: Geben Sie der Quarantäne einen aussagekräftigen Namen.

  Der **Ordnername** der Quarantäne bleibt unverändert. Er steht nur für einige, neu erstellte Quarantänen zur Verfügung.
- **Emails löschen nach**: Definieren Sie, wie viele Tage eine Email in der Quarantäne verbleibt, bevor sie automatisch gelöscht wird.
- **Größe der Textauszüge**: Geben Sie an, welche Menge an Text aus der Email (Nachrichtentext) in die Datenbank geschrieben werden soll. Wenn Sie diesen Wert eingeben, berücksichtigen Sie Datenschutzverpflichtungen und die erforderliche Größe der Datenbank.
- **Verarbeitungsprotokoll einbeziehen**: Protokolliert die Verarbeitung der Emails in dieser Quarantäne. Das ermöglicht Ihnen zum Beispiel, die Gründe für die Aufnahme einer Email in die Quarantäne zu verfolgen. Im Avira Monitor, können Sie auf die entsprechende Email zugreifen und das Verarbeitungsprotokoll, einschließlich detaillierter Informationen, auf der Registerkarte **Verarbeitungsprotokoll** einsehen.
- **Quarantäne ist geschäftskritisch**: Jeder Quarantänefehler wird dem Job zurückgeschrieben. Der Job wird dann beendet und die Fehlerroutine des Jobs gestartet. Die Bearbeitung der Email, zum Beispiel ob der Job die Email ignoriert oder sie in das Verzeichnis BADMAIL ablegt, ist abhängig von den vorgenommenen Einstellungen für "geschäftskritisch" im Job selbst.

  Solange der Quarantänefehler nicht behoben ist, wird der Fehler wiederholt dem Job zurückgeschrieben.

- Wenn der Job selbst nicht geschäftskritisch ist, schaltet er sich nach einer bestimmten Zeit ab und verarbeitet keine weiteren Emails.
- Wenn der Job geschäftskritisch ist, wird jede Email in den Bereich BADMAIL verschoben und solange nicht zugestellt, bis der Fehler behoben ist.

Unabhängig von der Einstellung geschäftskritisch, werden die Avira Exchange Security Administratoren per Email über häufig auftretende Fehler in der Quarantäne oder im Job benachrichtigt.

3. Klicken Sie **Sammelbenachrichtigung**, um eine Quarantäne-Sammelbenachrichtigung für diese Quarantäne zu konfigurieren.

   Wenn Sie Ihren Anwendern ermöglichen möchten, auf die Verarbeitung der Whitelist zuzugreifen, wählen Sie unter **Vorlagen Quarantäne-Sammelbenachrichtigung mit Whitelist-Unterstützung**.

Verwandte Themen:

Geschäftskritische Jobs - Seite 40

7.5.3 Beispiel einer geschäftskritischen Quarantäne

Beispiel: Ein Job prüft auf Viren und findet einen Virus in einer eingehenden Email. Der Job ist so konfiguriert, dass standardmäßig die Email nicht an den Empfänger sondern in die Quarantäne verschoben wird. Aufgrund eines Quarantänefehlers steht die Quarantäne jedoch nicht zur Verfügung. Daher kann die Email nicht in die Quarantäne verschoben werden.

Mögliche Einstellungen für die Quarantäne und den Job:

Die Quarantäne ist geschäftskritisch	Der Job ist geschäftskritisch	Ergebnis
nein	nein	Der Quarantänefehler wird ignoriert. Die Email kann zwar nicht in die Quarantäne kopiert werden, sie wird jedoch auch nicht zugestellt.
nein	ja	Der Quarantänefehler wird ignoriert. Die Email kann zwar nicht in die Quarantäne kopiert werden, sie wird jedoch auch nicht zugestellt.
ja	nein	Die Jobverarbeitung wird abgebrochen und die virulente(!) Email an den nächsten Job der Verarbeitungskette unbearbeitet übergeben.
ja	ja	Die Email wird in die BADMAIL-Quarantäne verschoben und dort

Die Quarantäne ist geschäftskritisch	Der Job ist geschäftskritisch	Ergebnis
		vorgehalten. Die Email wird nicht zugestellt.

7.5.4 Quarantäne-Zusammenfassungen

Quarantäne-Zusammenfassungen informieren über die Emails, die von Avira Exchange Security unter die Quarantäne gestellt worden sind.

Sammelbenachrichtigungen können an verschiedenste Empfänger/-gruppen gesendet werden und eine Liste verschiedenster Quarantäne-Emails enthalten. Welche Emails das sind, welche Aktion der Empfänger der Sammelbenachrichtigung für diese Emails starten kann und welche Zusatzinformationen die Sammelbenachrichtigung enthält, wird in jeder Sammelbenachrichtigung separat konfiguriert.

Hinweis
Für eine Verbindung zur Avira Exchange Quarantäne müssen Sie die Ports 8008 und 8009 in der Windows Firewall festlegen. Wenn diese Ports nicht offen sind, ist es nicht möglich, sich über die **Quarantäne-Sammelbenachrichtigung** mit Avira Exchange zu verbinden, um Anfragen oder Freigaben zu erwirken, oder um vertrauenswürdige Absender zur Whiteliste hinzuzufügen.

Jede Art der Benachrichtigungen besteht aus zwei Teilen:

- Aus der Vorlage, in der die Form der Sammelbenachrichtigung definiert wird. Die Vorlagen der Sammelbenachrichtigungen können unter **Basiskonfiguration** › **Allgemeine Einstellungen** › **Vorlagen** › **Quarantäne-Zusammenfassungen** bearbeitet werden. Die hier zur Verfügung stehenden Variablen stehen ausschließlich mit den Sammelbenachrichtigungen und deren Form in Zusammenhang.
- Aus einer Liste der in Quarantäne gestellten Emails (der eigentliche Inhalt der Sammelbenachrichtigung), in der mit Feldern definiert wird, welche Emails und Email-Felder in der erstellten Sammelbenachrichtigung aufgeführt werden sollen.

Der Inhalt der Sammelbenachrichtigung wird durch die Variable **Sammelbenachrichtigung: Liste der Quarantäne-Mails** (*[VAR]HTMLList[/VAR]*) definiert, die in jeder Sammelbenachrichtigung ein Pflichteintrag ist. Welche Einträge diese Liste enthält, wird unter **Basiskonfiguration** › **Ordner** › **Quarantäne** › **Eigenschaften einer Quarantäne** › **Sammelbenachrichtigungen** › **Hinzufügen** › **Felder** definiert.

Die Checkbox für den **Absender** in der Registerkarte **Felder** in einer Quarantäne bezeichnet den Absender der in Quarantäne gestellten Emails, welcher innerhalb der Liste der Emails aufgeführt wird.

Verwandte Themen:
Benachrichtigungsvorlagen erstellen - Seite 130

7.5.5 Sammelbenachrichtigung erstellen

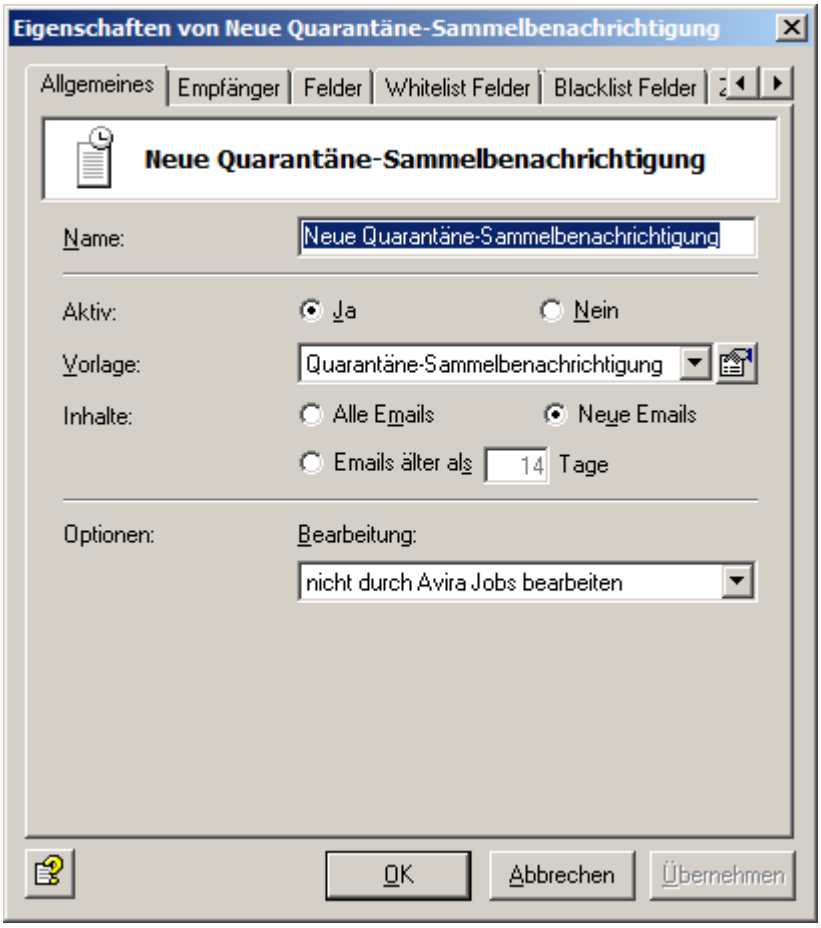
Sammelbenachrichtigungen sind vor allem für Quarantänen unerwünschter Emails und für die Empfänger dieser unerwünschten Emails bestimmt. Üblicherweise erhalten die Benutzer eine

Liste aller neuen unerwünschten Emails, die an sie adressiert waren und die in eine bestimmte Email-Quarantäne verschoben wurden.

Sie können für eine Quarantäne mehrere verschiedene Sammelbenachrichtigungen mit unterschiedlichem Inhalt erstellen. Die Emails werden für jede Sammelbenachrichtigung separat aus der Quarantäne zusammengetragen, selbst wenn der Zeitplan für diese Sammelbenachrichtigungen identisch ist.

Unter **Basiskonfiguration** › **Ordner** › **Quarantäne** erhalten Sie eine Liste aller Quarantänen. Anhand der Spalte **Sammelbenachrichtigung** erkennen Sie sofort, für welche Quarantänen eine Sammelbenachrichtigung konfiguriert ist (*ja/nein*).

1. Öffnen Sie **Basiskonfiguration** › **Ordner** › **Quarantäne**.
2. Öffnen Sie im rechten Fenster die Email-Quarantäne mit einem Doppelklick. Z. B. **Email Filter: Mittel**.
3. Auf der Registerkarte **Sammelbenachrichtigungen** klicken Sie **Hinzufügen**.
4. Passen Sie auf der Registerkarte **Allgemeines** die Einstellungen an.

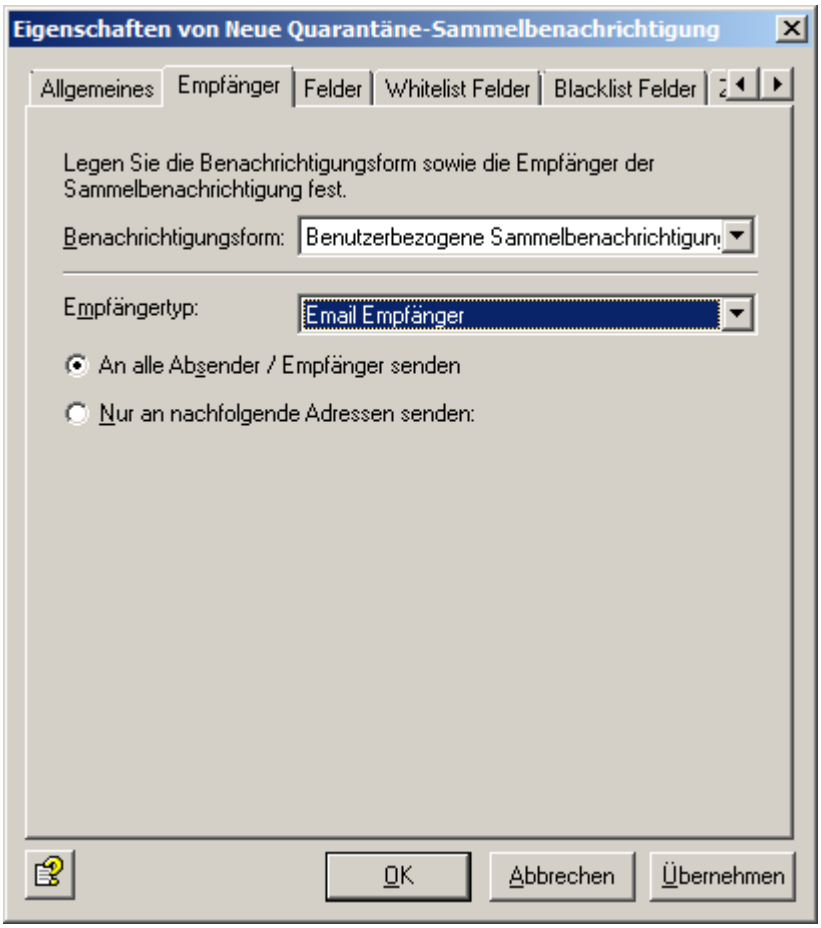


- **Name**: Vergeben Sie einen Namen für die Sammelbenachrichtigung und klicken Sie **Ja**, um die Benachrichtigung zu aktivieren.
- **Vorlage**: Wählen Sie eine von Ihnen unter **Allgemeine Einstellungen** › **Vorlagen** › **Quarantäne** › **Quarantäne-Sammelbenachrichtigungen** definierte

Sammelbenachrichtigung aus. Standardmäßig ist in Avira Exchange Security die Vorlage **Quarantäne-Sammelbenachrichtigung** vorhanden, die bereits vorkonfigurierte Einstellungen enthält. Wenn Sie Ihren Anwendern ermöglichen möchten, dass sie aus der Sammelbenachrichtigung heraus einen Absender auf ihre Benutzer-Whitelist setzen können, verwenden Sie die Vorlage **Quarantäne-Sammelbenachrichtigung mit Whitelist-Unterstützung**. Wenn Sie Ihren Anwendern ermöglichen möchten, dass sie aus der Sammelbenachrichtigung heraus einen Absender auf ihre Benutzer-Blacklist setzen können, verwenden Sie die Vorlage **Quarantäne-Sammelbenachrichtigung mit Blacklist-Unterstützung**.

- **Inhalte der Sammelbenachrichtigung**: Wählen Sie **Neue Mails**. Dadurch erhält der Empfänger der Sammelbenachrichtigung nur diejenigen Emails, die seit der letzten Sammelbenachrichtigung in die Quarantäne verschoben wurden.
- **Bearbeitung**: **nicht durch Avira Jobs bearbeiten** bedeutet, dass die erneut gesendete Email, die der Benutzer angefordert oder freigegeben hat, nicht mehr durch die aktiven Avira Jobs geprüft wird. Jede angeforderte oder freigegebene Email wird ungeprüft an die Empfänger zugestellt.

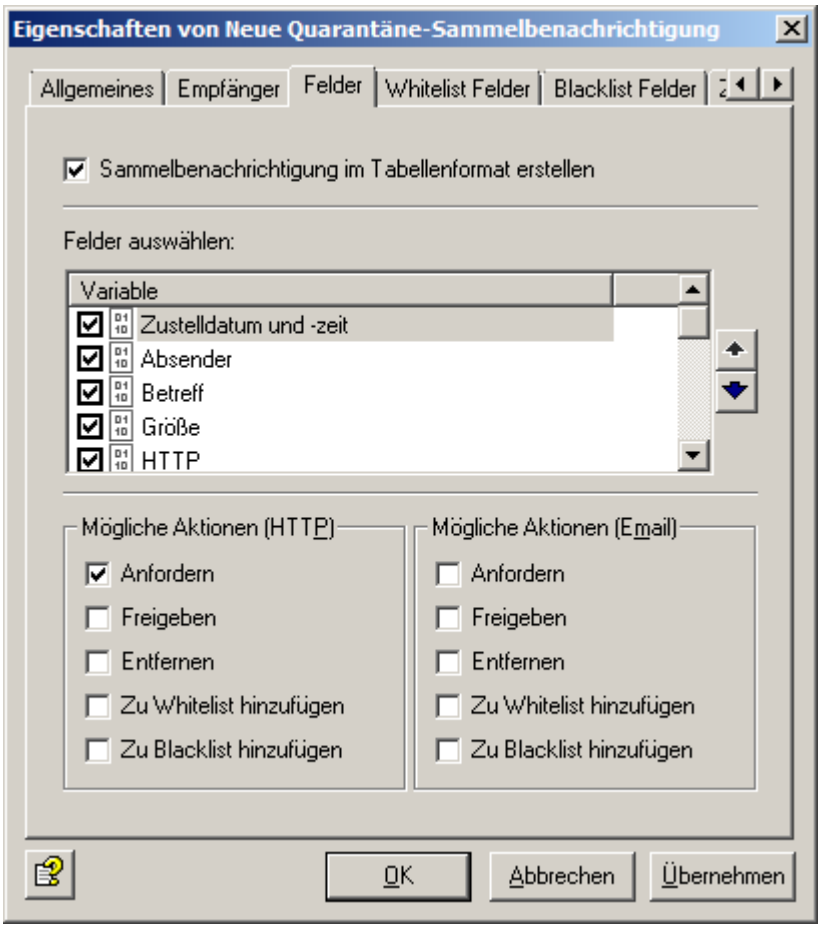
5. Wählen Sie auf der Registerkarte **Empfänger** Format und Adressen für die Sammelbenachrichtigung.



- **Administrative Sammelbenachrichtigung**: Alle Administratoren erhalten eine Sammelbenachrichtigung über die Quarantäne-Emails.

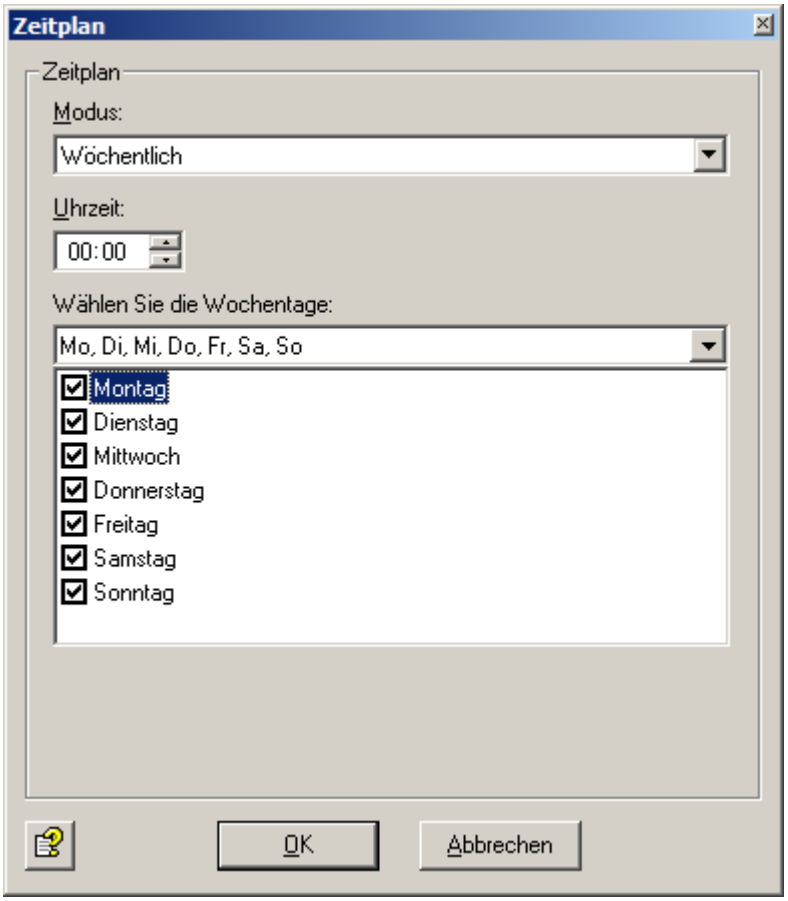
- **Benutzerdefinierte Sammelbenachrichtigung**: Definieren Sie, ob Empfänger oder Absender einer Email die Sammelbenachrichtigung erhalten sollen.
- **Benutzerdefinierte Empfänger**: Definieren Sie eine Gruppe von Empfängern, die eine Sammelbenachrichtigung erhalten sollen. Die ausgewählten Empfänger, Absender, Gruppen oder andere Adressmuster werden dann im unteren Textfeld aufgelistet.

6. Auf der Registerkarte **Felder** wählen Sie aus, welche Felder aus den Quarantäne-Emails in die Sammelbenachrichtigung geschrieben werden sollen.



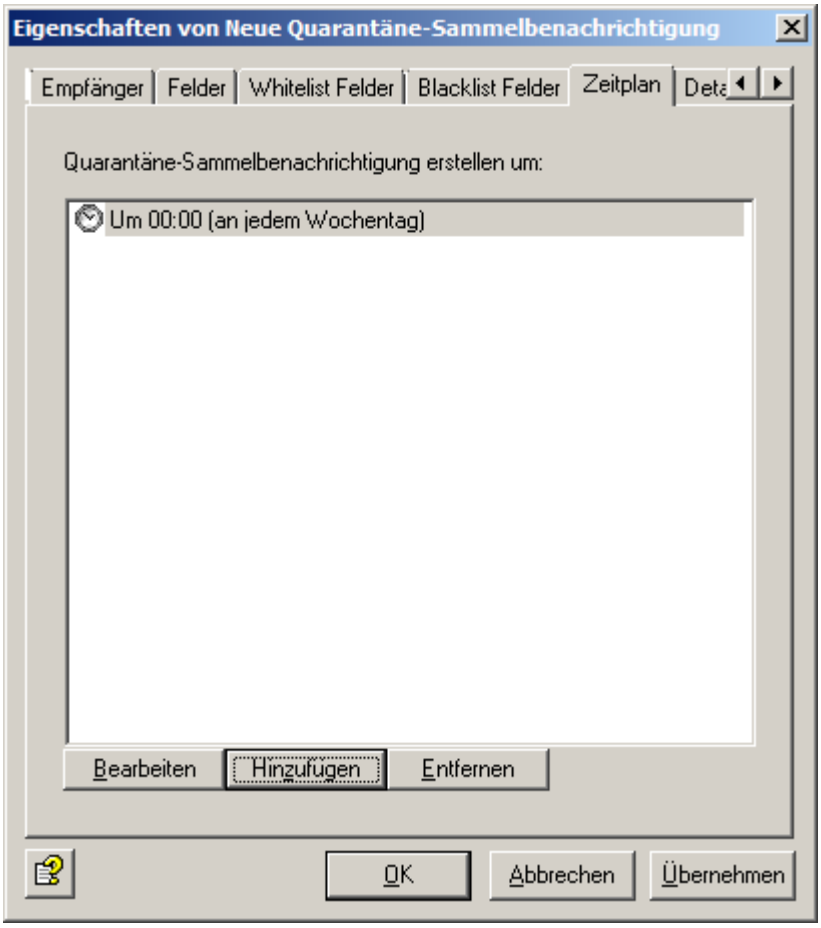
- **Variable**: Wählen Sie die Variablen aus, die der Benachrichtigung hinzugefügt werden sollen.
- **Links in der Benachrichtigung**: Wählen Sie die Aktionen, die ein Empfänger durch Klicken auf die Links in der Sammelbenachrichtigung ausführen darf.
  - **Anfordern**: Die Email wird dem Empfänger der Sammelbenachrichtigung aus der Quarantäne zugestellt.
  - **Freigeben**: Die Email wird allen ursprünglichen Empfängern der Email zugestellt.
  - **Entfernen**: Die Email wird in der Quarantäne zum Löschen vorgemerkt.
  - **Zu Whitelist hinzufügen**: Der Absender der Email wird zur Benutzer-Whitelist hinzugefügt.
  - **Zu Blacklist hinzufügen**: Der Absender der Email wird zur Benutzer-Blacklist hinzugefügt.

7. Auf der Registerkarte **Whitelist Felder** bzw. **Blacklist Felder** wählen Sie aus, welche Felder der Quarantäne-Emails in die Whitelist- bzw. Blacklist-Benachrichtigung aufgenommen werden sollen.
8. Klicken Sie auf die Registerkarte **Zeitplan** und dort auf **Hinzufügen**.



9. Im Dialog **Zeitplan** definieren Sie den Startzeitpunkt für die Erstellung der Sammelbenachrichtigung.
   Beispielsweise wird eine Sammelbenachrichtigung für die Quarantäne **Email Filter: Mittel** generiert und allen Empfängern jeden Wochentag um Mitternacht zugestellt.
10. Klicken Sie auf **OK**.

    Auf der Registerkarte **Zeitplan** wird Ihre neue Quarantäne-Sammelbenachrichtigung angezeigt.



Mit **Bearbeiten** ändern Sie die Zeit oder die Wochentage. Mit **Entfernen** löschen Sie die Sammelbenachrichtigung.

11. Klicken Sie **Übernehmen** und schließen Sie den Dialog **Eigenschaften**.

Verwandte Themen:

Liste der Benachrichtigungsvariablen - Seite 131

7.6 Utility-Einstellungen

- **Fingerprints**: Avira: Avira Exchange Security umfasst bei der Auslieferung eine in Kategorien eingeteilte umfangreiche Liste an Fingerabdrücken für die Erkennung von Dateitypen. Im Regelfall ist es nicht nötig, Änderungen vorzunehmen.
- **Wortlisten**: Sie können Wortlisten mit Zeichenfolgen erstellen, die Sie bei der Inhalts- und Email-Filterung mit Avira Email-Filter sperren möchten. Wir stellen verschiedene Kategorien für Wortlisten bereit, die Sie an Ihre Bedürfnisse anpassen können.
- **Avira Scan Engine**

Verwandte Themen:

Fingerprints - Seite 56
Wortlisten erstellen - Seite 74
Avira Scan Engine konfigurieren und aktivieren - Seite 35

Avira Email Filter

7.7 Konfiguration der Richtlinien-Konfiguration

In der **Richtlinien-Konfiguration** definieren Sie Ihre Avira-Jobs basierend auf firmeneigenen Richtlinien.

Anhand unterschiedlicher Bedingungen (oder auch Filter) können Sie festlegen, welche Emails überhaupt betroffen sind, wann welche Aktion ausgeführt werden soll und in welcher Reihenfolge die Jobs abgearbeitet werden sollen (Priorität). Alle Bedingungen können innerhalb der Jobs konfiguriert werden.

Die Summe der Avira-Jobs ergibt die Unternehmensrichtlinien (Policy).

7.7.1 Beispiel für eine Unternehmensrichtlinie

Jede eingehende Email mit unerwünschtem Inhalt soll erkannt, gelöscht oder in die Quarantäne verschoben werden.

Emails mit unerwünschtem Inhalt sollen den Empfänger zwar nicht erreichen, er soll aber darüber informiert werden, dass und welche Emails mit unerwünschtem Inhalt für ihn eingegangen sind, damit er selbst entscheiden kann, welche dieser Emails ihm doch zugestellt werden sollen. Dies soll über eine tägliche Sammelbenachrichtigung erfolgen.

Das alles können Sie in den Avira Filterung unerwünschter Emails -Jobs einrichten.

7.7.2 Jobarten

Es gibt mehrere unterschiedliche Jobtypen. Klicken Sie **Neu** im Kontextmenü unter **Richtlinien-Konfiguration** › **Mail-Transport-Jobs**.

Im Lieferumfang von Avira Exchange Security ist eine Reihe von Standardjobs enthalten, die Sie für Ihre Bedürfnisse ändern können. Selbstverständlich sind auch eigene Jobs möglich.

Sie finden die vorkonfigurierten Jobs unter **Richtlinien-Konfiguration** › **Jobvorlagen**. Ziehen Sie den gewünschten Job mit der Maus in **Mail-Transport-Jobs**.

Sie können beliebig viele Jobs anlegen.

Die Verarbeitungsreihenfolge der Jobs wird in der Ansicht aller Jobs in **Richtlinien-Konfiguration** › **Mail-Transport-Jobs** angezeigt. Neue Jobs werden am Ende der Liste hinzugefügt und können mit den Pfeiltasten in der Symbolleiste oder mit rechter Maustaste **Alle Aufgaben** › **Nach oben / Nach unten** an die gewünschte Position verschoben werden.

Ein Job kann aktiv oder inaktiv sein. Ein inaktiver Job ist zwar in der Konfiguration vorhanden, kommt aber nicht zur Ausführung. Sie müssen also Ihre Jobs nicht endgültig aus der Konfiguration löschen, wenn Sie diese deaktivieren wollen.

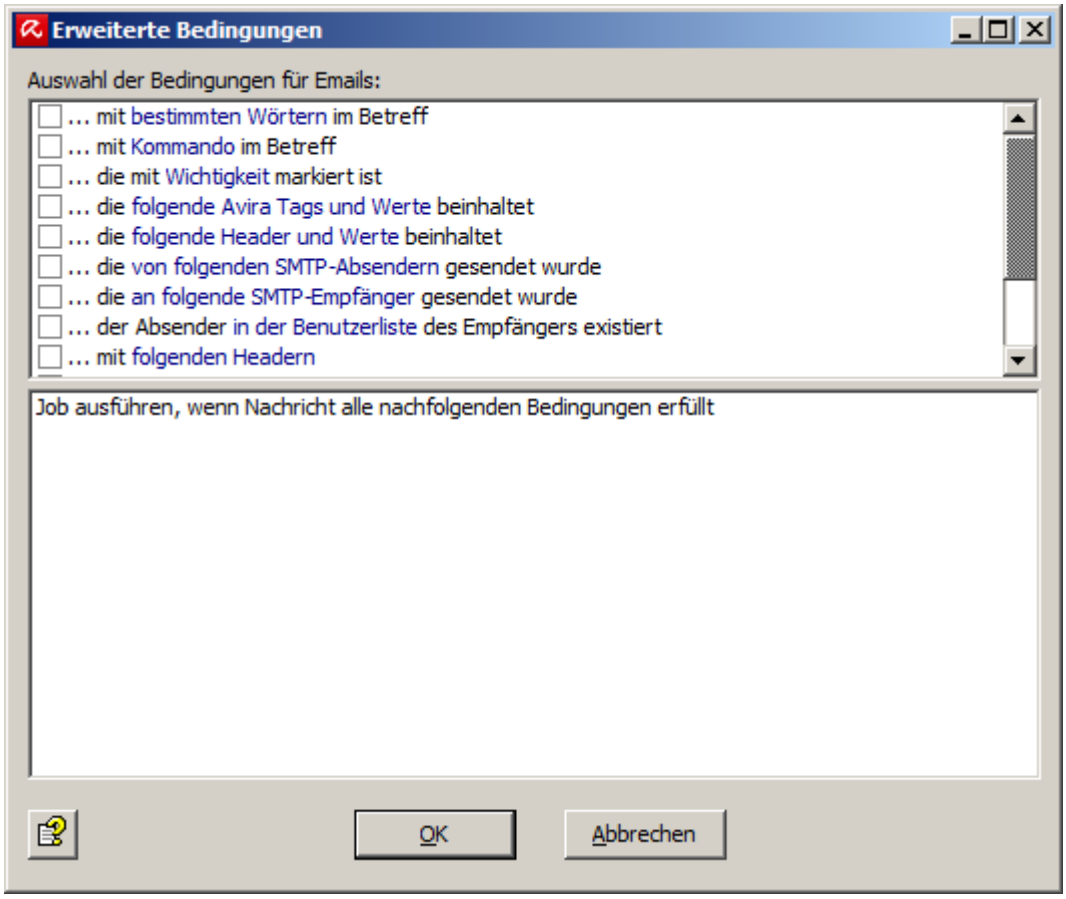
In jedem Job können Sie auf der Registerkarte **Aktionen** einstellen, welche Aktionen zur Ausführung kommen sollen, wenn eine Email unter die definierten Bedingungen fällt oder mit einem Virus infiziert ist.

Jobart	Beschreibung
Avira Prüfung	Job prüft die Emails auf Viren.
Avira Email-Größenfilterung	Job prüft die Emails auf eine maximal zugelassene Größe (Angabe pro Email).
Avira Anhangsfilterung	Job prüft die Emails auf verbotene Dateianhänge. Die verschiedenen Dateiformate werden durch Fingerprints identifiziert.
Avira Anhangs-/Größenfilterung	Job prüft die Emails auf verbotene Dateianhänge. Gleichzeitig kann die maximal zulässige Größe eines Anhangs angegeben werden.
Avira geschützte Anhangserkennung	Der Job reagiert auf Emails mit passwortgeschützten Archiven und führt die in der Registerkarte **Aktionen** konfigurierten Jobaktionen aus. Dadurch können passwortgeschützte Archive regelbasiert behandelt werden.
Avira Email-Filter Inhaltsfilterung	Job prüft Emails und Anhänge auf verbotenen Textinhalt.
Avira Email-Filter Adressfilterung	Job prüft Emails auf Adresseinschränkungen.
Avira Email-Filter Empfänger-Limit-Filterung	Job prüft Emails auf eine maximal zulässige Anzahl der Empfänger pro Email (gezählt werden die Empfänger im „To“- Feld einer Email).
Avira Filterung unerwünschter Emails	Job prüft Emails mittels verschiedener Kriterien auf unerwünschten Inhalt.

Adressenfilter können bei allen Jobarten konfiguriert werden. Sie können z. B. einen Job mit den Bedingungen erstellen, alle Emails, die von den Domänen **@gmx.net* und **@hotmail.com* gesendeSie können z. B. einen Job mit den Bedingungen erstellen, alle Emails, die von den Domänen *@gmx.net und *@hotmail.com gesendet werden, die größer als 500 KB sind, in denen der Betreff das Wort "Look" enthält und die der Fingerabdruck-Kategorie **Sound** angehören, zu löschen (und damit dem Empfänger nicht zuzustellen) und eine Kopie davon in die Quarantäne zu stellen. Dieser Fall wäre ein Avira Anhangs-/Größenfilterung-Job.

7.7.3 Job-Bedingungen

In jedem Job können Sie Voraussetzungen festlegen, die Emails aufweisen müssen, damit ein Job ausgeführt wird. Die Bedingungsparameter legen Sie gemäß Ihren Anforderungen selbst fest.


Erweiterte Bedingungen
Auswahl der Bedingungen für Emails:
... mit bestimmten Wörtern im Betreff
... mit Kommando im Betreff
... die mit Wichtigkeit markiert ist
... die folgende Avira Tags und Werte beinhaltet
... die folgende Header und Werte beinhaltet
... die von folgenden SMTP-Absendern gesendet wurde
... die an folgende SMTP-Empfänger gesendet wurde
... der Absender in der Benutzerliste des Empfängers existiert
... mit folgenden Headern
Job ausführen, wenn Nachricht alle nachfolgenden Bedingungen erfüllt
OK
Abbrechen

Nur wenn alle Voraussetzungen für eine versendete oder eintreffende Email gültig sind, wird eine Job-Verarbeitung initiiert, z.B. auf Viren geprüft.

Warnung
Die inhaltlichen Bedingungen müssen mit den definierten Adressbedingungen der Registerkarte **Adressen** übereinstimmen, damit der Job ausgeführt wird (*UND*-Verknüpfung).

Über den Wert von vorhandenen X-Headern kann die Email-Verarbeitung gesteuert werden. Externe Applikationen, welche die Emails vor der Verarbeitung durch Avira Exchange Security verarbeiten, können z.B. bestimmte X-Header-Felder mit definierten Werten in die Emails schreiben.

Sie können Jobs mithilfe der Bedingung **die folgenden Header und Werte beinhalten** so konfigurieren, dass in Abhängigkeit des Wertes eines X-Header-Feldes eine Job-Verarbeitung initiiert wird.

7.7.4 Job-Aktionen

Zusätzlich zu den Aktionen, die zur Funktion eines Jobs gehören, stehen Ihnen folgende Standard-Aktionen zur Verfügung.

Aktion	Bedeutung
Kopiere in Quarantäne	Eine Kopie der Email wird in den von Ihnen angegeben Quarantäne-Ordner gestellt, wo sie jederzeit eingesehen werden kann.
Lösche Email	Die infizierte/verbotene Original-Email wird endgültig vom Server gelöscht (die Kopie befindet sich in der Quarantäne, wenn die Option gesetzt ist).
Lösche Anhang	Die infizierten Anhänge werden endgültig vom Server gelöscht.
Zusatz im Betreff	Die Betreffzeile wird durch einen konfigurierbaren Zusatz ergänzt. Damit kann der Empfänger diese Email als bearbeitet identifizieren.
Sende Benachrichtigungen an	Benachrichtigungen können an folgende Personenkreise gesendet werden: • Administratoren • Absender • Empfänger • Andere
Starte externe Anwendung	Eine externe, frei wählbare Anwendung wird ausgeführt.
Header-Feld und Wert hinzufügen	Es wird im Header der Email ein Feld hinzugefügt, welches mit einem Wert aus den Variablen gefüllt werden kann.
Email umleiten	Die Email wird an die angegebenen Empfänger umgeleitet. Option: Original- Empfänger erhalten die E-Mail zusätzlich.
Header entfernen	Das Header-Feld wird aus der Email entfernt. Sie können dieser Aktion verwenden, wenn Sie die X-Header-Felder entfernen möchten, die vorher auf anderen Server festgelegt wurden.

8 Schaltflächen der Symbolleiste

Schaltfläche	Beschreibung
	Zurück
	Vorwärts
	Eine Ebene höher
	Eigenschaften des ausgewählten Objekts
	Aktualisieren
	Liste exportieren
	Hilfe
	Speichern
	Position/Rangfolge um eins hochsetzen
	Position/Rangfolge um eins heruntersetzen
	Job aktivieren
	Job deaktivieren
	Neues Objekt
	Filter in Quarantäne/Badmail setzen

9 Bedeutung der Symbole

Symbol	Beschreibung
	Avira Exchange Security Management Console Start und Logo
	Basiskonfiguration für die allgemeinen Einstellungen alles Module
	Knoten für Allgemeine Einstellungen
	Der Ordner für die Adresslisten
	Eine einzelne Avira Exchange Security Adressliste (Kragen rot), die mit Avira Exchange Security ausgeliefert wird und nicht geändert werden kann
	Eine einzelne benutzerdefinierte Adressliste (Kragen gelb), kann durch den Anwender erstellt werden und ist unter Eigenschaften konfigurierbar
	Der Ordner für Benachrichtigungsvorlagen, der die einzelnen Vorlagen für jeden Jobtyp und Empfänger enthält.
	Einzelne Benachrichtigungsvorlagen, unter Eigenschaften konfigurierbar
	Der Ordner für die einzelnen Datenbankverbindungen
	Das Symbol für eine einzelne Datenbankverbindung, unter Eigenschaften konfigurierbar
	Eine Liste aller Avira Exchange Security Server. Es lassen sich Server hinzufügen, entfernen und konfigurieren. Die gemeinsamen Eigenschaften aller Server werden unter **Allgemeine Einstellungen** > **Avira Server Einstellungen** konfiguriert, oder alternativ

Symbol	Beschreibung
	mit Klicken der rechten Maustaste auf **Avira Server** › **Eigenschaften**. Dazu gehören die Standard-Email-Adressen und die interne(n) Domäne(n)
	Allgemeine Avira Server Einstellungen unter dem Knoten Allgemeine Einstellungen im rechten Fenster.
	Ein einzelner Server, unter Eigenschaften konfigurierbar
	Ordner und Utility-Einstellungen. Unter Ordner finden Sie die Quarantänen, unter Utility-Einstellungen befinden sich alle zu konfigurierenden Zusätze wie Virenscanner, Fingerprints, Wortlisten.
	Die Quarantäne-Ordner-Struktur. Darunter befinden sich alle Quarantäne-Ordner.
	Ein einzelner Quarantäne-Ordner, unter Eigenschaften konfigurierbar. Die Quarantäne-Ordner enthalten die Original-Emails zur Überprüfung. Detaillierte Informationen können für jede Email abgerufen werden.
	Der Ordner für Fingerprint-Gruppen.
	Eine logisch zusammengehörende Fingerprint-Gruppe.
	Ein einzelner Fingerprint, unter Eigenschaften konfigurierbar
	Der Ordner für die Wortlisten, mit denen die Inhaltsprüfung durchgeführt wird
	Eine einzelne Wortliste, unter Eigenschaften konfigurierbar
	Der Avira Virenscanner, unter Eigenschaften konfigurierbar
	Richtlinien-Konfiguration für die Konfiguration von individuellen Jobs nach den eigenen Firmenrichtlinien.

Symbol	Beschreibung
	Ordner für Jobbeispiele, der die Jobs für die einzelnen Jobtypen enthält.
	Ein Avira Job oder Avira Email-Filter Job, von dem es verschiedene Jobtypen gibt, unter Eigenschaften konfigurierbar
	Ein aktiver Job, unter Eigenschaften konfigurierbar
	Ein inaktiver Job, unter Eigenschaften konfigurierbar
	Der Avira Monitor zur Einsicht in alle Quarantäne-Ordner auf jedem verfügbaren Server. Die Quarantäne-Ordner enthalten die Kopien der Original-Emails inklusive der Anhänge.
	Ein einzelnes Quarantäneobjekt
	Ungültiges Quarantäneobjekt
	Erneut gesendetes Quarantäneobjekt
	Information Store Quarantäneobjekt
	Uhrzeit und Wochentag einer Quarantäneaktualisierung
	Ordner für verschiedene, mit der Avira Exchange Security ausgelieferte Avira Reports
	Einzelner Avira Report

10 Supportinformationen

Support-Service

Auf unserer Webseite erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service:

www.avira.com/de/support

FAQ

Besuchen Sie auch den Bereich *Wissensdatenbank* auf unserer Webseite. Möglicherweise sind Ihre Fragen hier schon von anderen Benutzern gestellt und beantwortet worden.

Weitere Fragen zu Avira Produkten beantwortet Ihnen Ihr Avira Partner jederzeit gern.

Kontaktadresse

Kaplaneiweg 1, 88069 Tettnang, Deutschland

Internet

Weitere Informationen über uns und unsere Produkte finden Sie unter:

www.avira.com

Avira

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira Operations GmbH & Co. KG nicht gestattet.

Hier verwendete Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

Ausgabe Q4/2013

© 2013 Avira Operations GmbH & Co. KG. Alle Rechte vorbehalten.
Irrtümer und technische Änderungen vorbehalten.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | Telefon: +49 7542-500 0
www.avira.de